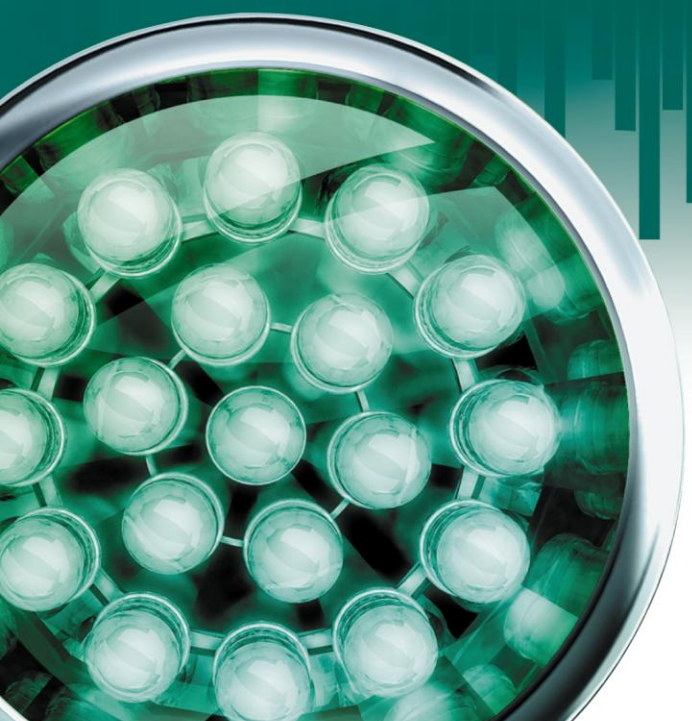
Kaspersky Internet Security 2011

USER GUIDE

APPLICATION VERSION: 11.0 CRITICAL FIX 1



KASPERSKY lab

Dear User!

Thank you for choosing our product. We hope that you will find this documentation useful and that it will provide answers to most of your questions that may arise.

Warning! This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction and distribution of this document or parts hereof will result in civil, administrative or criminal liability by applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document and related graphic images can be used exclusively for informational, non-commercial or personal use.

This document may be amended without additional notification. The latest version of this document can be found on the Kaspersky Lab website, at http://www.kaspersky.com/docs.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document for which the rights are held by third parties, or for any potential damages associated with the use of such documents.

This document uses registered trademarks and service marks, which are the property of their respective owners.

Document revision date: 06/24/2010

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved.

http://www.kaspersky.com
http://support.kaspersky.com

CONTENT

KASPERSKY LAB END USER LICENSE AGREEMENT 10

ABOUT THIS GUIDE 17

In this document 17

Document conventions 19

ADDITIONAL SOURCES OF INFORMATION 20

Sources of information for independent research 20

Discussing Kaspersky Lab applications on the web forum 21

Contacting the Sales Department 21

Contacting the Documentation development group 21

KASPERSKY INTERNET SECURITY 2011 22

What's new 22

Ensuring your computer protection 23

Distribution kit 25

Service for registered users 25

Hardware and software requirements 26

INSTALLING AND REMOVING THE APPLICATION 27

Standard installation procedure 27

Step 1. Finding a newer version of the application 28

Step 2. Making sure the system meets the installation requirements 28

Step 3. Select installation type 29

Step 4. Reviewing the license agreement 29

Step 5. Kaspersky Security Network Data Collection Statement 29

Step 6. Searching for incompatible applications 29

Step 7. Selecting the destination folder 30

Step 8. Preparing installation 30

Step 9. Installing 31

Step 10. Activating the application 31

Step 11. Registering a user 31

Step 12. Completing the activation 32

Step 13. System analysis 32

Step 14. Wizard completion 32

Updating the previous version of Kaspersky Internet Security 32

Step 1. Finding a newer version of the application 33

Step 2. Making sure the system meets the installation requirements 33

Step 3. Select installation type 34

Step 4. Reviewing the license agreement 34

Step 5. Kaspersky Security Network Data Collection Statement 34

Step 6. Searching for incompatible applications 34

Step 7. Selecting the destination folder 35

Step 8. Preparing installation 35

Step 9. Installing 36

Step 10. Completing the activation 36

Step 11. System analysis 36

Step 12. Wizard completion 36

Non-standard installation scenarios....36
Getting started....37
Removing the application....37
Step 1. Saving data for repeated use....38
Step 2. Confirmation of application removal....38
Step 3. Removing the application. Completing removal....38
MANAGING THE LICENSE....39
About End User License Agreement....39
About license....39
About activation code....40
Viewing license information....40
APPLICATION INTERFACE....42
Notification area icon....42
Context menu....43
Kaspersky Internet Security main window....44
Notification windows and pop-up messages....46
Application settings window....48
Kaspersky Gadget....49
STARTING AND STOPPING THE APPLICATION....50
Enabling and disabling automatic launch....50
Starting and stopping the application manually....50
COMPUTER PROTECTION STATUS....51
Diagnostics and elimination of problems in your computer protection....51
Enabling and disabling protection....53
Pausing and resuming protection....54
SOLVING TYPICAL TASKS....55
How to activate the application....55
How to purchase or renew a license....56
What to do when the application's notifications appear....57
How to update application databases and modules....57
How to scan critical areas of your computer for viruses....58
How to scan a file, folder, disk, or another object for viruses....59
How to perform full scan of your computer for viruses....60
Scanning computer for vulnerabilities....61
How to protect your personal data against theft....61
Protection against phishing....62
Virtual Keyboard....62
What to do if you suspect an object of being infected with a virus....63
What to do with a large number of spam messages....64
What to do if you suspect your computer of being infected....65
How to restore an object that has been deleted or disinfected by the application....67
How to create and use Rescue Disk....67
Create Rescue Disk....67
Starting the computer from the Rescue Disk....69
How to view the report on the application's operation....70
How to restore application default settings....70
Transferring Kaspersky Internet Security settings to the product installed on another computer....71

How to use Kaspersky Gadget 72
ADVANCED APPLICATION SETTINGS 74
General protection settings 75
Restricting access to Kaspersky Internet Security. 76
Selecting protection mode 76
Scan 77
Virus scan 77
Vulnerability Scan 84
Update 84
Selecting an update source 85
Creating the update startup schedule 87
Rolling back the last update 88
Scanning Quarantine after update 88
Using the proxy server 88
Running updates under a different user account 89
File Anti-Virus 89
Enabling and disabling File Anti-Virus 90
Automatically pausing File Anti-Virus 90
Creating a protection scope 91
Changing and restoring security level 92
Selecting scan mode 92
Using heuristic analysis 92
Selecting the scan technology 93
Changing actions to be performed on detected objects 93
Scan of compound files 93
Scan optimization 94
Mail Anti-Virus 95
Enabling and disabling Mail Anti-Virus 96
Creating a protection scope 96
Changing and restoring security level 97
Using heuristic analysis 97
Changing actions to be performed on detected objects 98
Attachment filtering 98
Scan of compound files 98
Email scanning in Microsoft Office Outlook 99
Email scanning in The Bat! 99
Web Anti-Virus 100
Enabling and disabling Web Anti-Virus 101
Selecting the Web Anti-Virus security level 102
Changing actions to be performed on dangerous objects 102
Checking URLs using the databases of suspicious and phishing addresses 102
Using heuristic analysis 103
Blocking dangerous scripts 104
Scan optimization 104
Kaspersky URL Advisor 104
Blocking access to dangerous websites 105
Control requests to regional domains 106
Controlling access to online banking services 106

Creating a list of trusted addresses....107
Restoring Web Anti-Virus default settings....107
IM Anti-Virus....107
Enabling and disabling IM Anti-Virus....108
Creating a protection scope....108
Selecting the scan method....108
Proactive Defense....109
Enabling and disabling Proactive Defense....110
Creating a group of trusted applications....110
Using the dangerous activity list....110
Changing the dangerous activity monitoring rule....110
System Watcher....111
Enabling and disabling System Watcher....111
Using patterns of dangerous activity (BSS)....112
Rolling back a malicious program's actions....112
Application Control....113
Enabling and disabling Application Control....113
Placing applications into groups....114
Viewing activity of applications....115
Modifying a trust group and restoring default group....115
Working with rules of Application Control....116
Protecting operating system resources and identity data....119
Interpreting the data of application usage by the participants of Kaspersky Security Network....120
Network protection....121
Firewall....121
Network Attack Blocker....126
Eencrypted connections scan....128
Network Monitor....130
Configuring the proxy server....130
Creating a list of monitored ports....131
Anti-Spam....132
Enabling and disabling Anti-Spam....134
Selecting spam protection level....135
Training Anti-Spam....135
Scanning links in messages....138
Detecting spam by phrases and addresses. Creating lists....138
Regulating threshold values of spam rate....144
Using additional features affecting the spam rate....144
Selecting the spam recognition algorithm....144
Adding a label to the message subject....145
Excluding Microsoft Exchange Server messages from the scan....145
Configuring spam processing by mail clients....146
Restoring the recommended Anti-Spam settings....148
Anti-Banner....148
Enabling and disabling Anti-Banner....149
Selecting the scan method....149
Creating the lists of blocked and allowed banner addresses....150
Exporting and importing the lists of addresses....150
Safe Run....151

Safe Run for Applications....152
Safe Run for Websites....155
Parental Control....156
Configuring user's Parental Control....157
Viewing reports of user's activity....165
Trusted zone....165
Creating a list of trusted applications....166
Creating the exclusion rules....167
Performance and compatibility with other applications....167
Selecting detectable threat categories....168
Advanced disinfection technology....168
Distributing computer resources when scanning for viruses....168
Running tasks in background mode....169
Application settings in full-screen mode. Gaming Profile....170
Battery saving....170
Kaspersky Internet Security self-defense....170
Enabling and disabling self-protection....171
Protection against external control....171
Quarantine and Backup....171
Storing quarantine and backup objects....172
Working with quarantined objects....172
Additional tools for better protection of your computer....174
Privacy Cleaner....175
Browser Configuration....176
Rolling back the changes, made by the wizards....177
Reports....178
Creating a report for the selected component....179
Data filtering....179
Events search....180
Saving a report to file....181
Storing reports....181
Clearing application reports....181
Logging non-critical events....182
Configuring the reminder of report availability....182
Application appearance....182
Application skin....182
Active interface elements....183
News Agent....183
Notifications....184
Enabling and disabling notifications....184
Configuring the notification method....184
Participating in the Kaspersky Security Network....185
VALIDATING KASPERSKY INTERNET SECURITY SETTINGS....187
Test "virus" EICAR and its modifications....187
Testing the HTTP traffic protection....188
Testing the SMTP traffic protection....189
Validating File Anti-Virus settings....189
Validating virus scan task settings....189

Validating Anti-Spam settings....190
CONTACTING THE TECHNICAL SUPPORT SERVICE....191
My Kaspersky Account....191
Technical support by phone....192
Creating a system state report....192
Creating a trace file....193
Sending data files....193
AVZ script execution....194
APPENDIX....196
Subscription statuses....196
Kaspersky Internet Security notifications list....198
Notifications in any protection mode....198
Notifications in interactive protection mode....204
Working with the application from the command line....215
Activating the application....216
Starting the application....217
Stopping the application....217
Managing application components and tasks....217
Virus scan....219
Updating the application....221
Rolling back the last update....222
Exporting protection settings....222
Importing protection settings....223
Creating a trace file....223
Viewing Help....224
Return codes of the command line....224
GLOSSARY....225
KASPERSKY LAB....234
INFORMATION ABOUT THIRD-PARTY CODE....235
Program code....235
AGG 2.4....237
ADOBE ABI-SAFE CONTAINERS 1.0....238
BOOST 1.39.0....238
BZIP2/LIBBZIP2 1.0.5....238
CONVERTUTF....238
CURL 7.19.4....239
DEELX - REGULAR EXPRESSION ENGINE 1.2....239
EXPAT 1.2, 2.0.1....239
FASTSCRIPT 1.90....240
FDLIBM 5.3....240
FLEX: THE FAST LEXICAL ANALYZER 2.5.4....240
FMT.H....240
GDTOA....240
GECKO SDK 1.8, 1.9, 1.9.1....241
ICU4C 4.0.1....249
INFO-ZIP 5.51....249
JSON4LUA 0.9.30....250

LIBGD 2.0.35 250
LIBJPEG 6B 251
LIBM (lrint.c v 1.4, lrintf.c,v 1.5) 252
LIBPNG 1.2.8, 1.2.9, 1.2.42 253
LIBUNGIF 3.0 253
LIBXDR 253
LREXLIB 2.4 254
LUA 5.1.4 254
LZMALIB 4.43 255
MD5.H 255
MD5.H 255
MD5-CC 1.02 255
OPENSSL 0.9.8K 256
PCRE 7.7, 7.9 257
SHA1.C 1.2 259
STLPORT 5.2.1 259
SVCCTL.IDL 259
TINYXML 2.5.3 259
VISUAL STUDIO CRT SOURCE CODE 8.0 259
WINDOWS TEMPLATE LIBRARY 8.0 260
ZLIB 1.0.4, 1.0.8, 1.2.2, 1.2.3 264
Development tools 264
MS DDK 4.0, 2000 264
MS WDK 6000, 6001, 6002 264
WINDOWS INSTALLER XML (WIX) TOOLSET 3.0 264
Distributed program code 268
GRUB4DOS 0.4.4-2009-10-16 (FILE GRUB.EXE) 269
SYSLINUX 3.86 (FILE SYSLINUX.EXE) 273
Other information 277
INDEX 278

KASPERSKY LAB END USER LICENSE AGREEMENT

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY ENTERING CORRESPONDING SYMBOL(-S) YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. **SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU**. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(-S) YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Definitions

1.1. Software means software including any Updates and related materials.

1.2. Rightholder (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.

1.3. Computer(s) means hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.

1.4. End User (You/Your) means individual(s) installing or using the Software on his or her own behalf or who is legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, *«You»* further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term *«organization,»* without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

1.5. Partner(s) means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.

1.6. Update(s) means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.

1.7. User Manual means user manual, administrator guide, reference book and related explanatory or other materials.

2. Grant of License

2.1. The Rightholder hereby grants You a non-exclusive license to store, load, install, execute, and display (to «use») the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the User Manual, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the «License») and you accept this License:

Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of computers specified in licenses you have obtained from the Rightholder *provided* that unless the licensing terms provide otherwise, each acquired license entitles you to install and use the Software on such a number of Computer(s) as is specified in Clauses 2.2 and 2.3.

2.2. If the Software was acquired on a physical medium You have the right to use the Software for protection of such a number of Computer(s) as is specified on the Software package.

2.3. If the Software was acquired via the Internet You have the right to use the Software for protection of such a number of Computers that was specified when You acquired the License to the Software.

2.4. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using the Software.

2.5. You can transfer the non-exclusive license to use the Software to other individuals within the scope of the license granted from the Rightholder to You provided that the recipient agrees to be bound by all the terms and conditions of this Agreement and substitute you in full in the license granted from the Rightholder. In case You fully transfer the rights granted from the Rightholder to use the Software You must destroy all copies of the Software including the back-up copy. If You are a recipient of a transferred license You must agree to abide by all the terms and conditions of this Agreement. If You do not agree to be bound by all the terms and conditions of this Agreement, You may not install and/or use the Software. You also agree as the recipient of a transferred license that You do not have any additional or better rights than what the original End User who acquired the Software from the Rightholder, did.

2.6. From the time of the Software activation or after license key file installation (with the exception of a trial version of the Software) You have the right to receive the following services for the defined period specified on the Software package (if the Software was acquired on a physical medium) or specified during acquisition (if the Software was acquired via the Internet):

- Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;

- Technical Support via the Internet and Technical Support telephone hotline.

3. Activation and Term

3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software or license key file installation. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Software installed and/or used on Your Computer.

3.2. If the Software was acquired on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement.

3.3. If the Software was acquired via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during acquisition.

3.4. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement *provided that* the trial version does not entitle You Updates and Technical support via the Internet and Technical support telephone hotline. If Rightholder sets another duration for the single applicable evaluation period You will be informed via notification.

3.5. Your License to Use the Software is limited to the period of time as specified in Clauses 3.2 or 3.3 (as applicable) and the remaining period can be viewed via means described in User Manual.

3.6. If You have acquired the Software that is intended to be used on more than one Computer then Your License to Use the Software is limited to the period of time starting from the date of activation of the Software or license key file installation on the first Computer.

3.7. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License to use the Software without refunding the purchase price or any part thereof.

3.8. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.

3.9. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.

3.10. The Rightholder reserves the right to limit the possibility of activation outside the region in which the Software was acquired from the Rightholder and/or its Partners.

3.11. If You have acquired the Software with activation code valid for language localization of the Software of that region in which it was acquired from the Rightholder or its Partners, You cannot activate the Software with applying the activation code intended for other language localization.

3.12. In case of limitations specified in Clauses 3.10 and 3.11 information about these limitations is stated on package and/or website of the Rightholder and/or its Partners.

4. Technical Support

4.1. The Technical Support described in Clause 2.6 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).

Technical support service: http://support.kaspersky.com

5. Information Collection

5.1. Having agreed with the terms and conditions of this Agreement You consent to provide information to the Rightholder about executable files and their checksums to improve Your security protection level.

5.2. In order to improve security awareness about new threats and their sources and in order to improve Your security protection level the Rightholder, with your consent, that has been explicitly confirmed in the Kaspersky Security Network Data Collection Statement, is expressly entitled to receives such information. You can deactivate the Kaspersky Security Network service during installation. Also, You can activate and deactivate the Kaspersky Security Network service at any time in the Software options page.

You further acknowledge and agree that any information gathered by Rightholder can be used to track and publish reports on security risk trends in the Rightholder's sole and exclusive discretion.

5.3. The Software does not process any personally identifiable data and does not combine the processing data with any personal information.

5.4. If you do not wish for the information collected by the Software to be sent to the Rightholder, You should not activate and/or de-activate the Kaspersky Security Network service.

6. Limitations

6.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

6.2. You shall not transfer the rights to use the Software to any third party except as set forth in Clause 2.5 of this Agreement.

6.3. You shall not provide the activation code and/or license key file to third parties or allow third parties access to the activation code and/or license key which are deemed confidential data of Rightholder and you shall exercise reasonable care in protecting the activation code and/or license key in confidence provided that you can transfer the activation code and/or license key to third parties as set forth in Clause 2.5 of this Agreement.

6.4. You shall not rent, lease or lend the Software to any third party.

6.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.

6.6. The Rightholder has the right to block the key file or to terminate Your License to use the Software in the event You breach any of the terms and conditions of this Agreement and without any refund to You.

6.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.

7. Limited Warranty and Disclaimer

7.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual provided however that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.

7.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.

7.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.

7.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.6 of this Agreement.

7.5. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in Clauses 3.2 or 3.3 of this Agreement or after the License to use the Software is terminated for any reason.

7.6. THE SOFTWARE IS PROVIDED «AS IS» AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY

FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE RIGHTHOLDER .

8. Exclusion and Limitation of Liability

8.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE RIGHTHOLDER AND/OR ITS PARTNERS ARE FOUND LIABILE, THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE RIGHTHOLDER OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

9. GNU and Other Third Party Licenses

9.1. The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code («Open Source Software»). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

10. Intellectual Property Ownership

10.1. You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners

(«Trademarks»). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.

10.2. You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

11. Governing Law; Arbitration

11.1. This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the Tribunal of International Commercial Arbitration at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 11 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

12. Period for Bringing Actions

12.1. No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

13. Entire Agreement; Severability; No Waiver

13.1. This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

14. Rightholder Contact Information

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd

Moscow, 123060

Russian Federation

Tel: +7-495-797-8700

Fax: +7-495-645-7939

E-mail: info@kaspersky.com

Web site: www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved. The Software and any accompanying documentation are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

ABOUT THIS GUIDE

This document is the Guide for installing, configuring and operating Kaspersky Internet Security 2011 (hereinafter Kaspersky Internet Security). The document is designed for a wide audience. Users of the application should be able to operate a personal computer at a basic level: to be familiar with the Microsoft Windows operating system interface and navigation within it, and to know how to use popular email and Internet programs, for example, Microsoft Office Outlook and Microsoft Internet Explorer.

The aim of the document:

- to help users to install the application on the computer on their own, and activate and configure it with regard to user's required tasks;
- to provide a readily available source of information on application related issues;
- to provide alternative sources of information about the application and the means of getting technical support.

IN THIS SECTION:

In this document 17

Document conventions 18

IN THIS DOCUMENT

This document contains the following sections:

Additional sources of information

This section contains a description of the data on the sources of additional information regarding the application and an Internet-resource where you can discuss the application, share ideas, ask questions and receive answers.

Kaspersky Internet Security 2011

This section describes the application's new features, and gives brief information about its individual components and basic functions. It reveals the function of each part of the package supplied and a range of services available to registered users of the application. This section contains hardware and software requirements which the computer must meet for the installation of Kaspersky Internet Security.

Installing and removing the application

This section contains instructions that help you install the application on your computer or update the previous version. This section also describes the application's uninstall procedure.

Managing the license

This section contains information regarding the basic concepts used in the context of the application licensing. In this section, you will also learn about the automatic renewal of the license and where to view information regarding the current license.

Application interface

This section contains a description of the basic GUI components of the application: icon and context menu, main application window, settings window, and notification windows.

Starting and stopping the application

This section contains information regarding the application's startup and shutdown.

Computer protection status

This section contains information about how to find out whether your computer is currently protected, or if its security is under threat, as well as how to eliminate emerging threats. In this section, you can also find information about enabling, disabling, and pausing protection when working with Kaspersky Internet Security.

Solving typical tasks

This section contains instructions on the basic tasks encountered by most users when working with the application.

Advanced application settings

This section provides detailed information about each application component and describes the operation and configuration algorithms for each component.

Checking the consistency of the application settings

This section contains recommendations in how to check if the application components run correctly.

Contacting the Technical Support Service

This section contains recommendations with respect for making contact with Kaspersky Lab from My Kaspersky Account on the Technical Support Service website and by phone.

Appendix

This section includes reference information which complements the document text.

Glossary

This section contains the list of terms used in the document and their definitions.

DOCUMENT CONVENTIONS

Document conventions used in this guide are described in the table below.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Please note that...	Warnings are highlighted in red and enclosed in frames. Warnings contain important information, for example, related to computer operations critical to its safety.
It is recommended to use...	Notes are enclosed in frames. Notes contain additional and reference information.
Example: ...	Examples are given by section, on a yellow background, and under the heading "Example".
Update means...	New terms are marked by italics.
ALT+F4	Names of keyboard keys appear in a bold typeface and are capitalized. Names of the keys followed by a "plus" sign indicate the use of a key combination.
Enable	Names of interface elements, for example, input fields, menu commands, buttons, etc., are marked in a bold typeface.
To configure a task schedule:	Instructions are marked by the arrow symbol. Instructions' introductory phrases are in italics.
`help`	Texts in the command line or texts of messages displayed on the screen have a special font.
<IP address of your computer>	Variables are enclosed in angle brackets. Instead of the variables the corresponding values are placed in each case, and the angle brackets are omitted.

ADDITIONAL SOURCES OF INFORMATION

If you have any questions regarding selecting, purchasing, installing or using Kaspersky Internet Security, various sources of information are available for your convenience. You can choose the most suitable information source, depending on the question level of importance and urgency.

IN THIS SECTION:

Sources of information for independent research 20

Discussing Kaspersky Lab applications on the web forum 21

Contacting the Sales Department 21

Contacting the Documentation development group 21

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

Kaspersky Lab provides the following sources of information about the application:

- application page on the Kaspersky Lab website;
- application page on the Technical Support Service website (in the Knowledge Base);
- FastTrack Support service page;
- help system.

Application page on the Kaspersky Lab website

This page (http://www.kaspersky.com/kaspersky_internet_security) provides you with general information on the application, its features and options.

Application page on the Technical Support Service website (Knowledge Base)

On this page (http://support.kaspersky.com/kis2011) you will find articles created by Technical Support Service specialists.

These articles contain useful information, advice and FAQs on purchasing, installing and using the application. They are sorted by subject, for example, Managing the license, Configuring Update, or Eliminating operation failures. The articles may provide answers to the questions that concern not only this application but other Kaspersky Lab products as well. The articles may also contain news from the Technical Support Service.

FastTrack Support service

On this service page, you can find the database of FAQs with answers regarding the application's operation. To use this service, you need an Internet connection.

To go to the service page, in the main application window, click the **Support** link and in the window that opens click the **FastTrack Support** button.

Help system

The application installation package includes the full and context help file. It contains information about how to manage computer protection (view protection status, scan various computer areas for viruses, and execute other

tasks). The full help and context help file provides you with information about all of the application's, listing and describing the settings and tasks related to each of them.

To open the help file, click the **Help** button in the required window, or press the **F1** key.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE WEB FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab specialists and other users in our forum at http://forum.kaspersky.com.

In this forum you can view existing topics, leave your comments, create new topics or use the search engine.

CONTACTING THE SALES DEPARTMENT

If you have questions about selecting or purchasing Kaspersky Internet Security or extending your license, you can contact the Sales Department http://www.kaspersky.com/contacts.

You can also send your questions to the Sales Department by email at sales@kaspersky.com.

CONTACTING THE DOCUMENTATION DEVELOPMENT GROUP

If you have any questions regarding documentation, have found an error or you would like to leave feedback, you can contact the Documentation development group. To contact the Documentation development group, send an email to docfeedback@kaspersky.com. Please use "Kaspersky Help Feedback: Kaspersky Internet Security" as the subject line in your message.

KASPERSKY INTERNET SECURITY 2011

This section describes the application's new features, and gives brief information about its individual components and basic functions. It reveals the function of each part of the package supplied and a range of services available to registered users of the application. This section contains hardware and software requirements which the computer must meet for the installation of Kaspersky Internet Security.

IN THIS SECTION:

What's new 22

Ensuring your computer protection 23

Distribution kit 25

Service for registered users 25

Hardware and software requirements 26

WHAT'S NEW

The following are new in Kaspersky Internet Security:

- New protection component of the System Monitor (see page 111) provides monitoring of applications activity in the system and provides detailed information to other protection components. Due to the recoverable history of the applications activity, the component can roll back the results of a malicious application's actions when such malicious actions are detected by various protection components.

- Advanced functionality of the Safe Run, *Safe Run for Applications* (see page 152), is an isolated desktop where you can launch suspicious applications without any harm to the main operating system.

- New modules have been added to improve Internet protection:

  - Safe Surf (see page 105) – includes the link scanning module known from the previous version of the application, and also may block access to insecure websites, which allows you staying in the safe Internet zone.

  - Geo Security (see page 106) – allows you to grant or deny access to websites based on their belonging to certain domains. This helps you, for example, to block access to websites which belong to regional domains with a high risk of infection.

- Application Control allows a more effective definition of applications statuses, as well as configuration of application rules using Kaspersky Security Network data based on the statistics of Application Control operation on many users' computers.

- With the help of the Idle Scan (see page 169) module the computer may be scanned for viruses while you are not working on it, then scanning will stop when you return to work. This allows you to perform a scan regularly and at the same time prevents a reduction in the computer running speed when you need it.

- The Parental Control (see page 156) functionality has been expanded: now you can control the user's access to the computer and Internet, the launch of computer applications, restrict access to websites with undesirable content and downloading files from the Internet, control user's communication in social networks and through Instant Messengers, as well as view reports on the controlled user's actions. To optimize the Parental Control configuration the module also includes an export and import option for the account with these settings.

- When using Kaspersky Internet Security on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can also use the Kaspersky Gadget (hereinafter *gadget*). Kaspersky Gadget is designed for quick access to the main features of the application: protection status indication, virus scan of objects, application operation reports, etc.

ENSURING YOUR COMPUTER PROTECTION

Kaspersky Internet Security provides comprehensive protection for your computer against known and emerging threats, network attacks and phishing, spam and other unwanted information.

Every type of threat is handled by an individual *protection component* (see the description of components in this section). Components can be enabled or disabled independently of one another and configured accordingly.

In addition to the constant protection provided by the security components, we recommend that you regularly *scan* your computer for viruses. This is necessary in order to rule out the possibility of spreading malicious programs that have not been discovered by security components, for example, because the security level was set to low or for other reasons.

To keep Kaspersky Internet Security up to date, you need to *update* the databases and software modules used by the application. The application is updated automatically by default. However, you can always update the databases and software modules manually, if necessary.

You can control the individual applications that are launched on your computer by using the *application activity control*. The way applications access *personal data* is subject to special control. These data include files, folders and registry keys, which contain the settings and important data of the most frequently used applications, as well as the user's files (My Documents folder, cookies, information about the user's activity). When the safety of any application raises doubts, they can be run in a *safe environment*.

Certain specific tasks that need to be performed occasionally can be performed with the help of advanced tools and wizards (see section "Additional tools for better protection of your computer" on page 174), such as configuring Microsoft Internet Explorer or erasing the traces of user activity in the system.

Protection components

The following protection components provide protection for your computer in real time:

File Anti-Virus

File Anti-Virus prevents infection of the computer's file system. The component starts upon startup of the operating system, continuously remains in the computer's RAM, and scans all files being opened, saved, or launched on your computer and all connected drives. Kaspersky Internet Security intercepts each attempt to access a file and scans the file for known viruses. The file can only be processed further if the file is not infected or is successfully treated by the application. If a file cannot be disinfected for any reason, it will be deleted. A copy of the file will be saved in the backup, or moved to quarantine.

Mail Anti-Virus

Mail Anti-Virus scans incoming and outgoing email messages on your computer. The email is available to the addressee only if it does not contain dangerous objects.

Web Anti-Virus

Web Anti-Virus intercepts and blocks scripts on websites if they pose a threat. All web traffic is also subject to a thorough monitoring. Additionally, the component blocks access to malicious websites.

IM Anti-Virus

IM Anti-Virus ensures the safe use of instant messengers. The component protects information that comes to your computer via IM protocols. IM Anti-Virus ensures safe operation of various applications for instant messaging.

Proactive Defense

Proactive Defense allows detection of a new malicious program before it can perform its malicious activity. The component's operation is based on monitoring and analyzing the behavior of all applications installed on your computer. Depending on the actions being performed, Kaspersky Internet Security makes a decision whether the application is potentially dangerous or not. So your computer is protected not only from known viruses, but also from new ones that have not yet been discovered.

Anti-Phishing

A component integrated in Web Anti-Virus, Anti-Spam and IM Anti-Virus, which checks web addresses to see if they are included in the list of phishing and suspicious web addresses.

Application Control

Application Control logs the actions performed by applications in the system, and manages the applications' activities, based on which group the component assigns them to. A set of rules is defined for each group of applications. These rules manage the applications' access to various operating system resources.

Firewall

The Firewall ensures security for your work in local networks and on the Internet. The component filters all network activities using two types of rule: *rules for applications* and *packet rules*.

Network Attack Blocker

The Network Attack Blocker loads during the operating system launch, and scans incoming network traffic for activities characteristic of network attacks. As soon as an attempt to attack the computer is detected, Kaspersky Internet Security blocks any network activity of the attacking computer towards your computer.

Anti-Spam

Anti-Spam integrates into the mail client installed on your computer, and monitors all incoming email messages for spam. All messages containing spam are marked with a special header. An option to configure Anti-Spam for spam processing (automatic removal, moving to a special folder, etc.) is also provided. The component also analyzes email messages to detect phishing.

Network Monitor

The component is designed for viewing information about network activity in real-time.

Anti-Banner

Anti-Banner blocks advertising information located on banners built into interfaces of various programs installed on your computer, or displayed online.

Parental Control

Parental Control functionality is designed to protect children and teenagers from threats associated with using the computer and Internet browsing.

Parental Control allows you set flexible restrictions on access to web resources and applications for different users depending on their age. It also lets you view statistical reports on controlled user activity.

There are three groups of objects protected by the application components:

- Files, identity data, user names and passwords, information about bank cards, etc. These files are protected by File Anti-Virus, Application Control and Proactive Defense.
- Applications installed on your computer and operating system objects. These files are protected by Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus, Application Control, Network Attack Blocker, Anti-Spam and Proactive Defense.

- Online activity: using e-payment systems, email protection against spam, viruses etc. These files are protected by Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus, Firewall, Network Attack Blocker, Anti-Spam, Network Monitor, Anti-Banner, Parental Control and Anti-Phishing.

The grouping of components depending on the objects they protect is graphically illustrated in the **Protection Center** section in the main application window (see section "Kaspersky Internet Security main window" on page 44).

DISTRIBUTION KIT

You can purchase the boxed version of Kaspersky Internet Security from our resellers, or purchase it online from Internet shops, such as the **eStore** section of http://www.kaspersky.com.

If you buy the boxed version of the program, the package will include:

- A sealed envelope with the installation CD containing the program files and documentation in PDF format.
- Documentation in printed form, notably Quick Start Guide and User Guide documents (depending on the region).
- License Agreement (depending on the region).
- Activation card containing an activation code (depending on the region).

Read the EULA through carefully (see section "About End User License Agreement" on page 39)!

If you do not agree with the terms of the EULA, you can return your boxed product to the reseller from whom you purchased it and be reimbursed the amount you paid for the program, provided that the envelope containing the installation disk is still sealed.

By opening the sealed installation disk, you accept all the terms of the EULA.

Before breaking the seal on the installation disk envelope, carefully read through the EULA.

If you buy Kaspersky Internet Security from eStore, you will download the product from the Kaspersky Lab website; the present User Guide is included with the installation package. You will be sent an activation code by email after your payment has been received.

SERVICE FOR REGISTERED USERS

Kaspersky Lab offers legal users a set of services that allow increased efficiency of the application use.

When you purchase the license, you become a registered user, which entitles you to benefit from the following services:

- hourly updated application database and new product versions;
- advice on how to install, configure, and use the product - by phone or in the Personal Cabinet;
- notification of new software products released by Kaspersky Lab and new viruses emerging all over the world. This service is provided to users who have subscribed to Kaspersky Lab's news delivery on the Technical Support Service website (http://support.kaspersky.com/subscribe).

Advice on issues related to the functioning and use of operating systems, third-party software, and various technologies are not provided.

HARDWARE AND SOFTWARE REQUIREMENTS

To ensure the proper functioning of Kaspersky Internet Security, a computer has to meet certain requirements.

General requirements:

- 480 MB of free disk space.
- CD / DVD-ROM (to install Kaspersky Internet Security from the distribution CD).
- Internet connection (to update databases and application modules).
- Microsoft Internet Explorer 6.0 or higher.
- Microsoft Windows Installer 2.0.

Requirements for Microsoft Windows XP Home Edition (Service Pack 2 or higher), Microsoft Windows XP Professional (Service Pack 2 or higher), Microsoft Windows XP Professional x64 Edition (Service Pack 2 or higher):

- Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent);
- 512 MB free RAM.

Requirements for Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:

- Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent);
- 1GB free RAM (32-bit); 2 GB free RAM (64-bit).

You cannot enable Safe Run when working under a Microsoft Windows XP (64-bit) operating system. Safe Run is restricted when working in Microsoft Windows Vista (64-bit) and Microsoft Windows 7(64-bit) operating systems.

Requirements for netbooks:

- Intel Atom 1.33 MHz (Z520) processor or a compatible equivalent.
- Intel GMA950 video card with video RAM of more than 64 MB (or a compatible equivalent).
- Screen size not less than 10.1".
- Microsoft Windows XP Home Edition or higher.

INSTALLING AND REMOVING THE APPLICATION

This section contains instructions that help you install the application on your computer or update the previous version. This section also describes the application's uninstall procedure.

IN THIS SECTION:

Standard installation procedure 27

Updating the previous version of Kaspersky Internet Security 32

Non-standard installation scenarios 36

Getting started 37

Removing the application 37

STANDARD INSTALLATION PROCEDURE

Kaspersky Internet Security will be installed on your computer in an interactive mode using the Setup Wizard.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

If the application will be used to protect more than one computer, it should be installed on all computers in the same way. Note that in this case, according to the license agreement, the license term begins from the date of the first activation.

- *To install Kaspersky Internet Security on your computer,*

  run the setup file (a file with the *.exe extension) from the CD containing the product.

Installation of Kaspersky Internet Security from a setup file downloaded online is identical to that from the installation CD.

IN THIS SECTION:

Step 1. Finding a newer version of the application 28

Step 2. Making sure the system meets the installation requirements 28

Step 3. Select installation type 29

Step 4. Reviewing the license agreement 29

Step 5. Kaspersky Security Network Data Collection Statement 29

Step 6. Searching for incompatible applications 29

Step 7. Selecting the destination folder 30

Step 8. Preparing installation 30

Step 9. Installing 31

Step 10. Activating the application 31

Step 11. Registering a user 31

Step 12. Completing the activation 32

Step 13. System analysis 32

Step 14. Wizard completion 32

STEP 1. FINDING A NEWER VERSION OF THE APPLICATION

Before setup, the Setup Wizard checks the update servers of Kaspersky Lab for a newer version of Kaspersky Internet Security.

If it does not find a newer product version on the Kaspersky Lab update servers, the Setup Wizard for the current version will be started.

If the update servers offer a newer version of Kaspersky Internet Security, you will see a prompt to download and install it on the computer. It is recommended that you install the new version of the application, because newer versions include more enhancements that allow you to ensure a more reliable protection of your computer. If you cancel the new version download, the Setup Wizard for the current version will be started. If you decide to install the newer version, product distribution files will be downloaded to your computer and the Setup Wizard for that new version will be started automatically. For a further description of the installation procedure for the newer version, please refer to its corresponding documentation.

STEP 2. MAKING SURE THE SYSTEM MEETS THE INSTALLATION REQUIREMENTS

Before installing Kaspersky Internet Security on your computer, the installer checks your operating system and service packs to make sure they meet the software requirements for installation (see section "Hardware and software requirements" on page 26). In addition, the installer checks the presence of required software and the credentials necessary to install applications. If any of the above-listed requirements is not met, the corresponding notification will be displayed on the screen.

If the computer meets all the requirements, the Wizard searches for Kaspersky Lab applications, which, when run together with Kaspersky Internet Security, may result in conflicts. If such applications are found, you are asked to remove them manually.

If an earlier version of Kaspersky Anti-Virus or Kaspersky Internet Security is found, all data that can be used by Kaspersky Internet Security 2011 (activation information, application settings, etc.) will be saved and used when installing the new application while the one installed earlier will be automatically removed.

STEP 3. SELECT INSTALLATION TYPE

At this stage, you can choose the most suitable type of Kaspersky Internet Security installation:

- *Standard installation*. If you choose this option (the **Change installation settings** box is unchecked), the application will be fully installed on your computer with protection settings recommended by Kaspersky Lab experts.
- *Custom installation*. In this case (the **Change installation settings** box is checked) you will be asked to specify the destination folder to which the application will be installed (see section "Step 7. Selecting the destination folder" on page 30), and disable the installation process protection, if required (see section "Step 8. Preparing installation" on page 30).

To proceed with the installation, click the **Next** button.

STEP 4. REVIEWING THE LICENSE AGREEMENT

At this stage, you should review the license agreement made between you and Kaspersky Lab.

Read the agreement carefully and give your consent by clicking the **I agree** button. The installation will continue.

If you cannot accept the license agreement, cancel the application installation by clicking the **Cancel** button.

STEP 5. KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

At this stage, you will be invited to participate in the Kaspersky Security Network. Participation in the program involves sending information about new threats detected on your computer, running applications, and downloaded signed applications to Kaspersky Lab, along with the unique ID assigned to your copy of Kaspersky Internet Security and your system information. We guarantee that none of your personal data will be sent.

Review the Kaspersky Security Network Data Collection Statement. To read the complete version of the Statement, click the **Full KSN agreement** button. If you agree with all points of the statement, check the **I accept the terms of participation in Kaspersky Security Network** box in the Wizard window.

Click the **Next** button when carrying out the custom installation (see section "Step 3. Select installation type" on page 29). When performing the standard installation, click the **Install** button. The installation will continue.

STEP 6. SEARCHING FOR INCOMPATIBLE APPLICATIONS

At this step, the application checks whether any applications incompatible with Kaspersky Internet Security are installed on your computer.

If no such applications are found, the Wizard automatically proceeds to the next step.

If any incompatible applications are detected, they are displayed in a list on the screen, and you are offered to remove them. Applications that Kaspersky Internet Security cannot remove automatically should be removed manually. While removing incompatible applications, you will need to reboot your operating system, after which installation of Kaspersky Internet Security will continue automatically.

To proceed with the installation, click the **Next** button.

STEP 7. SELECTING THE DESTINATION FOLDER

This step of the Setup Wizard is only available if the custom installation is selected (see section "Step 3. Select installation type" on page 29). For the standard installation, this step is omitted and the application is installed to the default folder.

At this stage you are asked to choose the folder to which Kaspersky Internet Security will be installed. The following path is set by default:

- **<disk>\Program Files\Kaspersky Lab\Kaspersky Internet Security 2011** – for 32-bit systems;
- **<disk>\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security 2011** – for 64-bit systems.

To install Kaspersky Internet Security to a different folder, specify the path to the required folder in the input field or click the **Browse** button and choose a folder in the window that opens.

Keep in mind the following restrictions:

- The application cannot be installed on network or removable drives, or on virtual drives (drives created using the `SUBST` command).
- We recommend that you avoid installing the application in a folder that already contain files or other folders, because access to that folder for editing will soon be blocked.
- The path to the installation folder cannot be longer than 160 characters or contain special characters **/**, **?**, **:**, *****, **"**, **>**, **<** and **|**.

To find out if there is enough disk space on your computer to install the application, click the **Volume** button. In the window that opens you can view the disk space information. To close the window, click **OK**.

To proceed with the installation, click the **Next** button in the Wizard window.

STEP 8. PREPARING INSTALLATION

This step of the Setup Wizard is only available if the custom installation is selected (see section "Step 3. Select installation type" on page 29). In the case of the standard installation, this step is skipped.

Since your computer may be infected with malicious programs that may impact the installation of Kaspersky Internet Security, the installation process should be protected.

By default, installation process protection is enabled – the **Protect the installation process** box is checked in the Wizard window.

You are advised to uncheck this box if the application cannot be installed (for example, when performing remote installation using Windows Remote Desktop). Enabled protection may be the reason.

In this case, you should interrupt the installation, restart it, check the **Change installation settings** box at the Select installation type step (see section "Step 3. Select installation type" on page 29), and, when reaching the Preparing installation step, uncheck the **Protect the installation process** box.

To proceed with the installation, click the **Install** button.

When installing the application on a computer running under Microsoft Windows XP, active network connections are terminated. The majority of terminated connections are restored after a pause.

STEP 9. INSTALLING

Installation of the application can take some time. Wait for it to complete.

Once the installation is complete, the Wizard will automatically proceed to the next step.

If an installation error occurs, due to malicious programs that prevent anti-virus applications from being installed on your computer, the Setup Wizard will prompt you to download *Kaspersky Virus Removal Tool utility*, a special tool for neutralizing an infection.

If you agree to install the utility tool, the Setup Wizard downloads it from Kaspersky Lab servers, after which installation of the utility starts automatically. If the Wizard cannot download the utility, you will be asked to download it on your own by clicking the link provided.

After you finish working with the utility, you should delete it and restart the installation of Kaspersky Internet Security.

STEP 10. ACTIVATING THE APPLICATION

Activation is the procedure of activating a license that allows you to use a fully functional version of the application until the license expires.

You will need an Internet connection to activate the application.

You will be offered the following options of Kaspersky Internet Security activation:

- **Activate commercial version**. Select this option and enter the activation code (see section "About activation code" on page 40) if you have purchased a commercial version of the application.

  If you specify an activation code for Kaspersky Anti-Virus in the entry field, the procedure of switching to Kaspersky Anti-Virus starts after the completion of activation.

- **Activate trial version**. Use this activation option if you want to install the trial version of the application before making the decision to purchase a commercial version. You will be able to use the fully-functional version of the application for the duration of a term limited by the license for the trial version of the application. When the license expires, it cannot be activated for a second time.

- **Activate later**. If you choose this option, the Kaspersky Internet Security activation stage is skipped. The application will be installed on your computer with the availability of all its functions, except updates. You will only be able to update anti-virus databases and modules of Kaspersky Internet Security once after installation. The **Activate later** option is only available at the first start of the Activation Wizard, immediately after installing the application.

STEP 11. REGISTERING A USER

This step is only available when activating the commercial version of the application. When activating the trial version, this step is skipped.

You need to register in order to be able to contact Kaspersky Lab Technical Support Service in the future.

If you agree to register, specify your registration data in the corresponding fields and click the **Next** button.

STEP 12. COMPLETING THE ACTIVATION

The Wizard informs you that Kaspersky Internet Security has been successfully activated. Additionally, information about the license is provided: license type (commercial or trial), date of expiry, and number of hosts for the license.

If you have activated the subscription, information about the subscription status (see section "Subscription statuses" on page 196) is displayed instead of the license expiration date.

Click the **Next** button to proceed with the Wizard.

STEP 13. SYSTEM ANALYSIS

At this stage, information about Microsoft Windows applications is collected. These applications are added to the list of trusted applications which have no restrictions imposed on the actions they perform in respect of the system.

Once the analysis is complete, the Wizard will automatically proceed to the next step.

STEP 14. WIZARD COMPLETION

The last window of the Wizard informs you of the successful completion of the application installation. To run Kaspersky Internet Security, make sure that the **Start Kaspersky Internet Security** box is checked, and click the **Finish** button.

In some cases, you may need to reboot your operating system. If the **Start Kaspersky Internet Security** box is checked, the application will be automatically run after you reboot your operating system.

If you have unchecked the box before closing the Wizard, you should run the application manually (see section "Starting and stopping the application manually" on page 50).

UPDATING THE PREVIOUS VERSION OF KASPERSKY INTERNET SECURITY

If Kaspersky Internet Security 2010 is already installed on your computer, you should update the application to Kaspersky Internet Security 2011. If you have an active license for Kaspersky Internet Security 2010, you will not have to activate the application: the Installation Wizard will automatically receive the information about your license for Kaspersky Internet Security 2010 to use it during the installation process.

Kaspersky Internet Security will be installed on your computer in an interactive mode using the Setup Wizard.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

If the application will be used to protect more than one computer, it should be installed on all computers in the same way. Note that in this case, according to the license agreement, the license term begins from the date of the first activation.

- *To install Kaspersky Internet Security on your computer,*

  run the setup file (a file with the *.exe extension) from the CD containing the product.

  Installation of Kaspersky Internet Security from a setup file downloaded online is identical to that from the installation CD.

IN THIS SECTION:

Step 1. Finding a newer version of the application 33

Step 2. Making sure the system meets the installation requirements 33

Step 3. Select installation type 34

Step 4. Reviewing the license agreement 34

Step 5. Kaspersky Security Network Data Collection Statement 34

Step 6. Searching for incompatible applications 34

Step 7. Selecting the destination folder 35

Step 8. Preparing installation 35

Step 9. Installing 36

Step 10. Completing the activation 36

Step 11. System analysis 36

Step 12. Wizard completion 36

STEP 1. FINDING A NEWER VERSION OF THE APPLICATION

Before setup, the Setup Wizard checks the update servers of Kaspersky Lab for a newer version of Kaspersky Internet Security.

If it does not find a newer product version on the Kaspersky Lab update servers, the Setup Wizard for the current version will be started.

If the update servers offer a newer version of Kaspersky Internet Security, you will see a prompt to download and install it on the computer. It is recommended that you install the new version of the application, because newer versions include more enhancements that allow you to ensure a more reliable protection of your computer. If you cancel the new version download, the Setup Wizard for the current version will be started. If you decide to install the newer version, product distribution files will be downloaded to your computer and the Setup Wizard for that new version will be started automatically. For a further description of the installation procedure for the newer version, please refer to its corresponding documentation.

STEP 2. MAKING SURE THE SYSTEM MEETS THE INSTALLATION REQUIREMENTS

Before installation of Kaspersky Internet Security on your computer, the installer checks the operating system and service packs to make sure they meet the software requirements for product installation (see section "Hardware and software requirements" on page 26). In addition, the installer checks the presence of required software and the credentials necessary to install applications. If any of the above-listed requirements is not met, the corresponding notification will be displayed on the screen.

If the computer meets all the requirements, the Wizard searches for Kaspersky Lab applications, which, when run together with Kaspersky Internet Security, may result in conflicts. If such applications are found, you are asked to remove them manually.

If an earlier version of Kaspersky Anti-Virus or Kaspersky Internet Security is found, all data that can be used by Kaspersky Internet Security 2011 (activation information, application settings, etc.) will be saved and used when installing the new application while the one installed earlier will be automatically removed.

STEP 3. SELECT INSTALLATION TYPE

At this stage, you can choose the most suitable type of Kaspersky Internet Security installation:

- *Standard installation*. If you choose this option (the **Change installation settings** box is unchecked), the application will be fully installed on your computer with protection settings recommended by Kaspersky Lab experts.

- *Custom installation*. In this case (the **Change installation settings** box is checked) you will be asked to specify the destination folder to which the application will be installed (see section "Step 7. Selecting the destination folder" on page 30), and disable the installation process protection, if required (see section "Step 8. Preparing installation" on page 30).

To proceed with the installation, click the **Next** button.

STEP 4. REVIEWING THE LICENSE AGREEMENT

At this stage, you should review the license agreement made between you and Kaspersky Lab.

Read the agreement carefully and give your consent by clicking the **I agree** button. The installation will continue.

If you cannot accept the license agreement, cancel the application installation by clicking the **Cancel** button.

STEP 5. KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

At this stage, you will be invited to participate in the Kaspersky Security Network. Participation in the program involves sending information about new threats detected on your computer, running applications, and downloaded signed applications to Kaspersky Lab, along with the unique ID assigned to your copy of Kaspersky Internet Security and your system information. We guarantee that none of your personal data will be sent.

Review the Kaspersky Security Network Data Collection Statement. To read the complete version of the Statement, click the **Full KSN agreement** button. If you agree with all points of the statement, check the **I accept the terms of participation in Kaspersky Security Network** box in the Wizard window.

Click the **Next** button when carrying out the custom installation (see section "Step 3. Select installation type" on page 29). When performing the standard installation, click the **Install** button. The installation will continue.

STEP 6. SEARCHING FOR INCOMPATIBLE APPLICATIONS

At this step, the application checks whether any applications incompatible with Kaspersky Internet Security are installed on your computer.

If no such applications are found, the Wizard automatically proceeds to the next step.

If any incompatible applications are detected, they are displayed in a list on the screen, and you are offered to remove them. Applications that Kaspersky Internet Security cannot remove automatically should be removed manually. While removing incompatible applications, you will need to reboot your operating system, after which installation of Kaspersky Internet Security will continue automatically.

To proceed with the installation, click the **Next** button.

STEP 7. SELECTING THE DESTINATION FOLDER

This step of the Setup Wizard is only available if the custom installation is selected (see section "Step 3. Select installation type" on page 29). For the standard installation, this step is omitted and the application is installed to the default folder.

At this stage you are asked to choose the folder to which Kaspersky Internet Security will be installed. The following path is set by default:

- **<disk>\Program Files\Kaspersky Lab\Kaspersky Internet Security 2011** – for 32-bit systems;
- **<disk>\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security 2011** – for 64-bit systems.

To install Kaspersky Internet Security to a different folder, specify the path to the required folder in the input field or click the **Browse** button and choose a folder in the window that opens.

Keep in mind the following restrictions:

- The application cannot be installed on network or removable drives, or on virtual drives (drives created using the `SUBST` command).
- We recommend that you avoid installing the application in a folder that already contain files or other folders, because access to that folder for editing will soon be blocked.
- The path to the installation folder cannot be longer than 160 characters or contain special characters **/**, **?**, **:**, *****, **"**, **>**, **<** and **|**.

To find out if there is enough disk space on your computer to install the application, click the **Volume** button. In the window that opens you can view the disk space information. To close the window, click **OK**.

To proceed with the installation, click the **Next** button in the Wizard window.

STEP 8. PREPARING INSTALLATION

This step of the Setup Wizard is only available if the custom installation is selected (see section "Step 3. Select installation type" on page 29). In the case of the standard installation, this step is skipped.

Since your computer may be infected with malicious programs that may impact the installation of Kaspersky Internet Security, the installation process should be protected.

By default, installation process protection is enabled – the **Protect the installation process** box is checked in the Wizard window.

You are advised to uncheck this box if the application cannot be installed (for example, when performing remote installation using Windows Remote Desktop). Enabled protection may be the reason.

In this case, you should interrupt the installation, restart it, check the **Change installation settings** box at the Select installation type step (see section "Step 3. Select installation type" on page 29), and, when reaching the Preparing installation step, uncheck the **Protect the installation process** box.

To proceed with the installation, click the **Install** button.

When installing the application on a computer running under Microsoft Windows XP, active network connections are terminated. The majority of terminated connections are restored after a pause.

STEP 9. INSTALLING

Installation of the application can take some time. Wait for it to complete.

Once the installation is complete, the Wizard will automatically proceed to the next step.

If an installation error occurs, due to malicious programs that prevent anti-virus applications from being installed on your computer, the Setup Wizard will prompt you to download *Kaspersky Virus Removal Tool utility*, a special tool for neutralizing an infection.

If you agree to install the utility tool, the Setup Wizard downloads it from Kaspersky Lab servers, after which installation of the utility starts automatically. If the Wizard cannot download the utility, you will be asked to download it on your own by clicking the link provided.

After you finish working with the utility, you should delete it and restart the installation of Kaspersky Internet Security.

STEP 10. COMPLETING THE ACTIVATION

The Wizard informs you that Kaspersky Internet Security has been successfully activated. Additionally, information about the license is provided: license type (commercial or trial), date of expiry, and number of hosts for the license.

If you have activated the subscription, information about the subscription status (see section "Subscription statuses" on page 196) is displayed instead of the license expiration date.

Click the **Next** button to proceed with the Wizard.

STEP 11. SYSTEM ANALYSIS

At this stage, information about Microsoft Windows applications is collected. These applications are added to the list of trusted applications which have no restrictions imposed on the actions they perform in respect of the system.

Once the analysis is complete, the Wizard will automatically proceed to the next step.

STEP 12. WIZARD COMPLETION

The last window of the Wizard informs you of the successful completion of the application installation. To run Kaspersky Internet Security, make sure that the **Start Kaspersky Internet Security** box is checked, and click the **Finish** button.

In some cases, you may need to reboot your operating system. If the **Start Kaspersky Internet Security** box is checked, the application will be automatically run after you reboot your operating system.

If you have unchecked the box before closing the Wizard, you should run the application manually (see section "Starting and stopping the application manually" on page 50).

NON-STANDARD INSTALLATION SCENARIOS

This section describes application installation scenarios which differ from those of standard installation or update from the previous version.

Installing Kaspersky Internet Security with further activation using an activation code of Kaspersky Anti-Virus

If, when installing Kaspersky Internet Security, at the Activating the application step, you enter an activation code of Kaspersky Anti-Virus, the switching procedure starts, which results in installing Kaspersky Anti-Virus on your computer.

If, when installing Kaspersky Internet Security, at the Application activation step, you select **Activate later** and then activate the application using an activation code of Kaspersky Anti-Virus, the switching procedure also starts, which results in installing Kaspersky Anti-Virus on your computer.

Installing Kaspersky Internet Security 2011 over Kaspersky Anti-Virus 2010

If you run the installation of Kaspersky Internet Security 2011 on a computer on which Kaspersky Anti-Virus 2010 with an active license is already installed, the Installation Wizard detects the information about the license and offers you to select one of the following further actions:

- Use the current license of Kaspersky Anti-Virus 2010. In this case, the switching procedure starts, which results in installing Kaspersky Anti-Virus 2011 on your computer. You will be able to use Kaspersky Anti-Virus 2011 still the license for Kaspersky Anti-Virus 2010 remains valid.

- Proceed with installation of Kaspersky Internet Security 2011. In this case, the installation procedure will be proceeded with according to the standard scenario, starting from the Activating the application step.

GETTING STARTED

The application is ready to be used after installation. To ensure proper protection of your computer, we recommend performing the following immediately after installation and configuration:

- Update application databases (see section "How to update application databases and modules" on page 57).

- Scan your computer for viruses (see section "How to perform full scan of your computer for viruses" on page 60) and vulnerabilities (see section "Scanning computer for vulnerabilities" on page 61).

- Check the protection status of your computer (on page 51) and eliminate protection problems if necessary (see section "Diagnostics and elimination of problems in your computer protection" on page 51).

REMOVING THE APPLICATION

After uninstalling Kaspersky Internet Security, your computer and personal data will be unprotected.

Kaspersky Internet Security is uninstalled with the help of the Setup Wizard.

To start the Wizard:

1. In the **Start** menu select **Programs** → **Kaspersky Internet Security 2011** → **Repair or Remove**.

2. In the window that opens, click the **Remove** button.

IN THIS SECTION:

Step 1. Saving data for repeated use 38

Step 2. Confirmation of application removal 38

Step 3. Removing the application. Completing removal 38

STEP 1. SAVING DATA FOR REPEATED USE

At this point you can specify which of the data used by the application you want to retain for repeated use during the next installation of the application (e.g., a newer version of the application).

By default, the application is completely removed from the computer.

To save data for repeated use, perform the following:

1. Select **Save application objects**.

2. Check the boxes opposite the data types you want to save:

   - **Activation data** – data that eliminates the need to activate the application in the future by automatically using the current license as long as it does not expire by the time of the next installation.

   - **Anti-Spam databases** – databases containing signatures of spam messages downloaded and saved by the application.

   - **Backup and Quarantine files** – files checked by the application and placed into backup storage or quarantine.

   - **Operational settings of the application** – values of the application settings selected during configuration.

   - **iSwift and iChecker data** – files which contain information about the objects that have already been scanned for viruses.

   - **Safe Run shared folder data** – files saved by the application working in a safe environment in a special folder that is also accessible in the normal environment.

STEP 2. CONFIRMATION OF APPLICATION REMOVAL

Since removing the application threatens the security of the computer and your personal data, you will be asked to confirm your intention to remove the application. To do this, click the **Remove** button.

To stop removal of the application at any time, you can cancel this operation by clicking the **Cancel** button.

STEP 3. REMOVING THE APPLICATION. COMPLETING REMOVAL

At this step, the Wizard removes the application from your computer. Wait until removal is complete.

When removing the application, your operating system may require reboot. If you cancel immediate reboot, completion of the removal procedure will be postponed until the operating system is rebooted, or the computer is turned off and then restarted.

MANAGING THE LICENSE

This section contains information regarding the basic concepts used in the context of the application licensing. In this section, you will also learn about the automatic renewal of the license and where to view information regarding the current license.

IN THIS SECTION:

About End User License Agreement 39

About license 39

About activation code 40

Viewing license information 40

ABOUT END USER LICENSE AGREEMENT

The *End User License Agreement* – is an agreement between natural or legal person lawfully in possession of a copy of an application. The EULA is included in each Kaspersky Lab application. It contains a detailed description of rights and Kaspersky Internet Security usage restrictions.

According to the EULA, when you purchase and install a Kaspersky Lab application, you get an unlimited right to own its copy.

ABOUT LICENSE

License is a right to use Kaspersky Internet Security and the related additional services offered by Kaspersky Lab or its partners.

Each license is defined by its expiry date and a type.

License term – a period during which the additional services are offered:

- technical support;
- updating databases and application modules.

The services provided depend on the license type.

The following license types are provided:

- *Trial* – a free license with a limited validity period, for example, 30 days, offered to become familiar with Kaspersky Internet Security.

  A trial license can only be used once and cannot be used after a commercial license!

  A trial license is supplied with the trial version of the application. If you have a trial license, you can only contact Technical Support Service if your question is about activating the product or purchasing a commercial license. As soon as the trial license expires, all Kaspersky Internet Security features become disabled. To continue using the application, you should activate it (see section "How to activate the application" on page 55).

- *Commercial* – a commercial license with a limited validity period (for example, one year), offered upon purchase of Kaspersky Internet Security. One license can cover several computers.

  If a commercial license is activated, all application features and additional services are available.

  As soon as a commercial license expires, Kaspersky Internet Security remains a full-featured application, but the anti-virus databases are not updated. You can still scan your computer for viruses and use the protection components, but only using the databases that you had when the license expired. Two weeks before the license expiration date, the application will notify you of this event so you can renew the license in advance (see section "How to purchase or renew a license" on page 56).

- *Commercial with an update subscription* and *commercial with an update and protection subscription* – a paid license with flexible management: you can suspend and resume the subscription, extend its validity period in the automatic mode and cancel the subscription. A license with subscription is distributed by service providers. You can manage the subscription from the user's Personal Cabinet on the service provider's website.

  The validity period of a subscription can be limited (for example, to one year) or unlimited. If a subscription with a limited validity period is activated, you should renew it on your own when it expires. A subscription with an unlimited validity period is extended automatically subject to timely prepayment to the provider.

  If the subscription term is limited, when it expires, you will be offered a grace period for subscription renewal, during which the full functionality of the program will be maintained.

  If the subscription is not renewed, when grace period expires, Kaspersky Internet Security ceases to update the application databases (for licenses with an update subscription) and stops performing computer protection or executing scan tasks (for licenses with a protection subscription).

  When using the subscription, you will not be able to use another activation code to renew the license. This is only possible after the subscription expiry date.

  If already have an activated license with a limited term at the time of subscription activation, it is substituted with the subscription license. To cancel the subscription, contact the service provider from whom you purchased Kaspersky Internet Security.

Depending on the subscription provider, the set of available actions to take on the subscription (see section "Subscription statuses" on page 196) may vary. Also, the grace period when subscription renewal is available, is not provided by default.

ABOUT ACTIVATION CODE

Activation code is the code supplied with a Kaspersky Internet Security commercial license. This code is required for activation of the application.

The activation code represents a sequence of Latin characters and digits separated by hyphens into four groups of five symbols without spaces. For example, 11111-11111-11111-11111.

VIEWING LICENSE INFORMATION

To view information about the active license:

1. Open the main application window.

2. Click the **License** button in the bottom part of the window to open the **License management** window.

In this window, you can start the application activation (see section "How to activate the application" on page 55), purchase a new license, or renew your current one (see section "How to purchase or renew a license" on page 56).

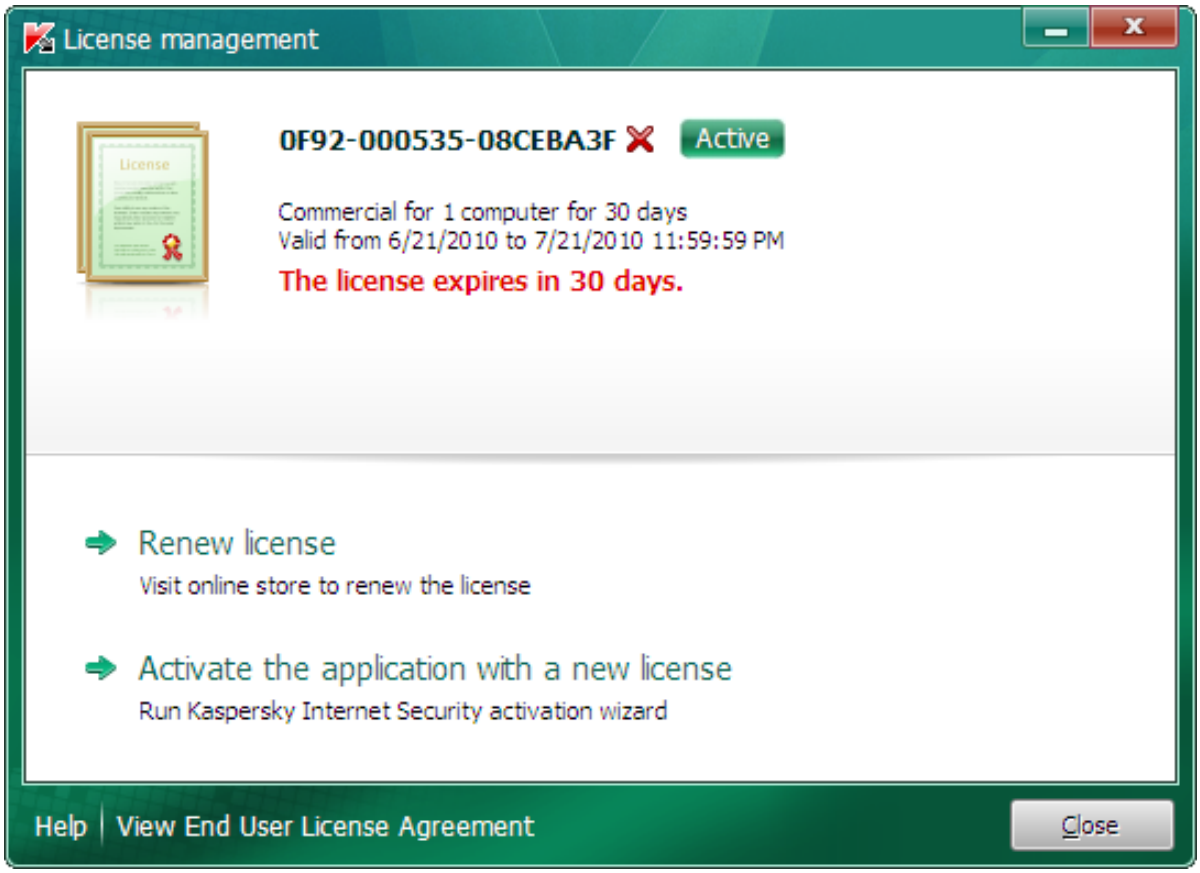

License management
0F92-000535-08CEBA3F
Active
Commercial for 1 computer for 30 days
Valid from 6/21/2010 to 7/21/2010 11:59:59 PM
The license expires in 30 days.
Renew license
Visit online store to renew the license
Activate the application with a new license
Run Kaspersky Internet Security activation wizard
Help
View End User License Agreement
Close

Figure 1. The License management window

APPLICATION INTERFACE

Kaspersky Internet Security has a fairly simple and easy-to-use interface. This section discusses its basic features in detail.

Kaspersky Internet Security includes extension components (plug-ins) for Microsoft Office Outlook, Microsoft Outlook Express, The Bat!, Thunderbird, Mozilla Firefox, Microsoft Internet Explorer and Microsoft Windows Explorer. The plug-ins expand the functionality of the host applications, providing access to the configuration of product components within their interface.

IN THIS SECTION:

Notification area icon 42

Context menu 43

Kaspersky Internet Security main window 44

Notification windows and pop-up messages 46

Application settings window 48

Kaspersky Gadget 49

NOTIFICATION AREA ICON

Immediately after installing the application, the application icon appears in the Microsoft Windows taskbar notification area.

In the Microsoft Windows 7 operating system the application icon is hidden by default, but you can display it to access the application more easily (see the operating system documentation).

The icon has the following basic purposes:

- It is an indicator of the application's operation.
- It provides access to the context menu, main application window and the news window.

Indication of the application activity

This icon serves as an indicator of the application's operation. It also indicates the protection status and shows a number of basic functions currently being performed by the application:

– scanning an email message;

– scanning web traffic;

– updating databases and application modules;

– computer needs to be restarted to apply updates;

– a failure occurred in the operation of an application component.

The icon is animated by default: for example, during the email message scan, a tiny letter symbol blinks against the application icon; when the update is in progress, you can see a revolving globe. You can deactivate animation (see section "Active interface elements" on page 183).

When the animation is disabled, the icon can take the following form:

(colored symbol) – all or certain protection components are activated;

(black-and-white symbol) – all protection components are disabled.

Access to the context menu and application windows

You can use the icon to open the context menu (on page 43) and the main application window (see section "Kaspersky Internet Security main window" on page 44).

To open the context menu,

hover the cursor over the icon and right-click the area.

To open the main application window,

hover the cursor over the icon and left-click the area.

If news from Kaspersky Lab is available, the icon appears in the Microsoft Windows taskbar notification area. Double-click this icon to open News Agent window (see section "News Agent" on page 183).

CONTEXT MENU

You can run basic protection tasks from the context menu.

The Kaspersky Internet Security menu contains the following items:

- **Update** – runs the update of application databases and modules.
- **Tools** – opens a submenu containing the following items:
  - **Application Control** – opens the **Applications Activity** window;
  - **Network Monitor** – opens the **Network Monitor** window;
  - **Virtual Keyboard** – displays the Virtual Keyboard.
- **Safe Run for Applications** – runs the safe desktop for handling applications that you suspect of being malicious. If Safe Run for Applications is already active, the application switches to it.

  When working with Safe Run for Applications, this menu item is named **To the main**, being used for switching to the main desktop.
- **Kaspersky Internet Security** – opens the main application window.
- **Pause protection / Resume protection** – temporarily turns off / on the real-time protection components. This menu item does not affect the application's updates, or the execution of virus scans.
- **Enable Parental Control / Disable Parental Control** – enables / disables Parental Control for the current account.
- **Setting** – opens the application settings window.
- **About** – opens a window containing information about the application.

- **News** – opens the news agent window (see section "News Agent" on page 183). This menu item is displayed if there is unread news.

- **Exit** – close Kaspersky Internet Security (when this item is selected, the application is unloaded from the computer's RAM).

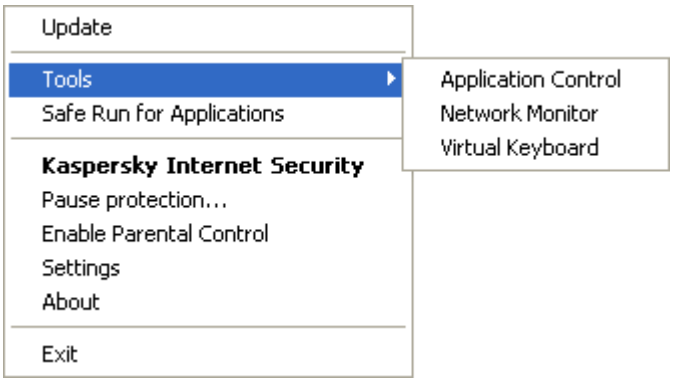


Figure 2. Context menu

If a virus scan or update task is running at the moment that you open the context menu, its name as well as its progress status (percentage complete) is displayed in the context menu. When you select a menu item with the name of a task, you can switch to the main window with a report of current task run results.

To open the context menu,

hover over the application icon in the taskbar notification area with the cursor and right-click it with the mouse.

In the Microsoft Windows 7 operating system the application icon is hidden by default, but you can display it to access the application more easily (see the operating system documentation).

KASPERSKY INTERNET SECURITY MAIN WINDOW

The main application window contains interface elements that provide access to all the main features of the application.

The main window can be divided into three parts:

- The top part of the window contains the protection status indicator which informs you of your current computer protection status.

Figure 3. Current computer protection status

There are three possible protection status values: each one is indicated by a color. Green indicates that your computer's protection is at the correct level, while yellow and red indicate that there are various security threats. In addition to malicious programs, threats include obsolete application databases, disabled protection components, the selection of minimum protection settings etc.

Security threats must be eliminated as they appear (see section "Diagnostics and elimination of problems in your computer protection" on page 51).

- The left part of the window allows you to quickly switch to the main application features: enabling and disabling protection components, running virus scan tasks, updating databases and program modules, etc.

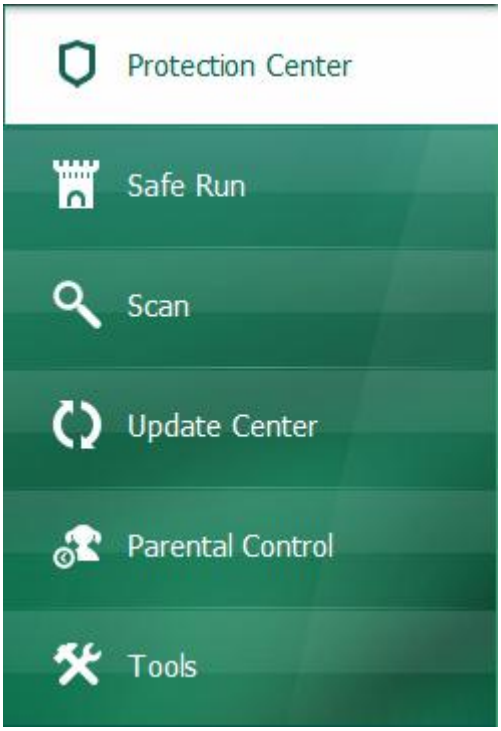


Figure 4. Left part of the main window

- The right part of the window contains information about the application function selected in the left part, and allows configuration of its settings, provides tools for executing virus scan tasks, retrieving updates etc.

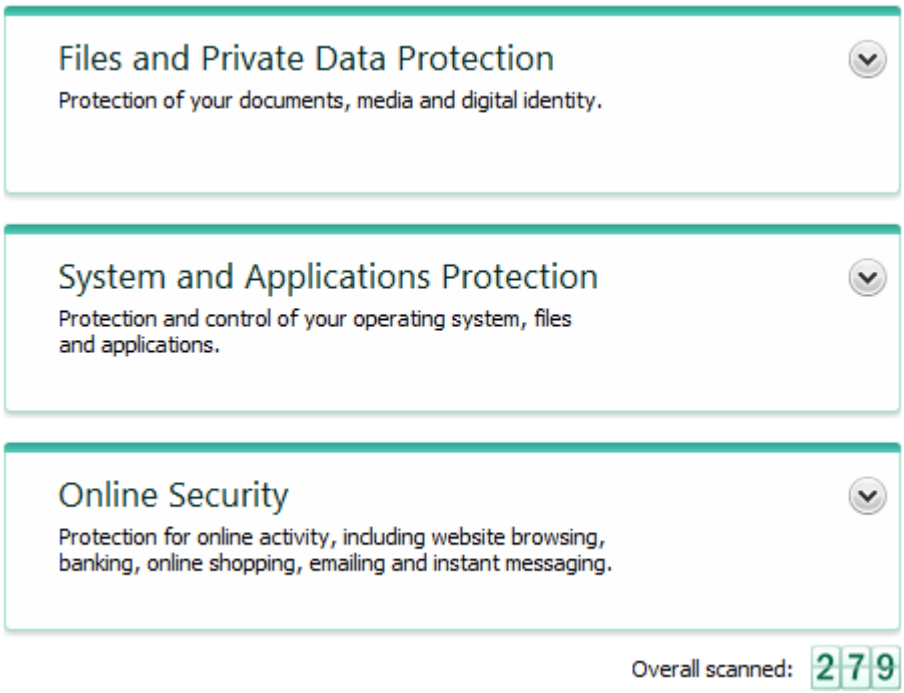

Files and Private Data Protection
Protection of your documents, media and digital identity.
System and Applications Protection
Protection and control of your operating system, files and applications.
Online Security
Protection for online activity, including website browsing, banking, online shopping, emailing and instant messaging.
Overall scanned: 279

Figure 5. Right part of the main window

You can also use the following buttons and links:

- **Settings** – to open the application settings window.
- **Quarantine** – to start working with quarantined objects.
- **Reports** – switch to the application operation report in diagram format.
- **News** – switch to viewing news in the News Agent window (see section "News Agent" on page 183). This link is displayed after the application receives a piece of news.
- **Help** – to view the Kaspersky Internet Security help system.
- **My Kaspersky Account** – to enter the user's personal account on the Technical Support Service website (see section "My Kaspersky Account" on page 191).
- **Support** – to open the window containing information about the system and links to Kaspersky Lab information resources (Technical Support Service website, forum).
- **License** – Kaspersky Internet Security activation, license renewal.

You can change the appearance of Kaspersky Internet Security using alternate skins (see section "Application appearance" on page 182).

To open the main application window, perform one of the following actions:

- hover the cursor over the application icon in the taskbar notification area and left-click it with the mouse.

  In the Microsoft Windows 7 operating system the application icon is hidden by default, but you can display it to access the application more easily (see the operating system documentation).

- select **Kaspersky Internet Security** from the context menu (see section "Context menu" on page 43);
- click the Kaspersky Internet Security icon located in the center of Kaspersky Gadget (only for Microsoft Windows Vista and Microsoft Windows 7).

NOTIFICATION WINDOWS AND POP-UP MESSAGES

Kaspersky Internet Security notifies you of important events occurring during its operation, using *notification windows* and *pop-up messages* that appear over the application icon in the taskbar notification area.

Notification windows are displayed by Kaspersky Internet Security when various actions can be taken in connection with an event: for example, if a malicious object is detected, you can block access to it, delete, or try to disinfect it. The application offers you to select one of the available actions. A notification window only disappears from the screen if you select one of the actions.

Kaspersky Internet Security 2011
Help
Virus Scan
Removable drive connected
You are advised to scan it for malicious software
Do you want to scan the removable drive?
Quick Scan
Only potentially dangerous files will be scanned
Full Scan
All files on the removable drive will be scanned
Do not scan
The removable drive will not be scanned
Always perform in such cases

Figure 6. The Notifications window

Pop-up messages are displayed by Kaspersky Internet Security in order to inform you of events that do not require selection of an action. Some pop-up messages contain links that you can use to take an action offered by the application: for example, run the update of the databases, or initiate the activation of the application). Pop-up messages automatically disappear from the screen soon after they appear.

Figure 7. Pop-up message

Depending on how critical the event is for computer security, you might receive the following types of notification:

- Critical notifications – inform you of events of critical importance from the viewpoint of computer security: for example, detection of a malicious object or dangerous activity in the system. Notification windows and pop-up messages of this type are red-colored.
- Important notifications – inform you of events which are potentially important from the viewpoint of computer security: for example, detection of a potentially infected object or suspicious activity in the system. Notification windows and pop-up messages of this type are yellow-colored.
- Information notifications – inform you of events that are non-critical from the viewpoint of security. Notification windows and pop-up messages of this type are green-colored.

APPLICATION SETTINGS WINDOW

The Kaspersky Internet Security settings window is designed for configuring the entire application, separate protection components, scan and update tasks, and for running other advanced configuration tasks (see section "Advanced application settings" on page 74).

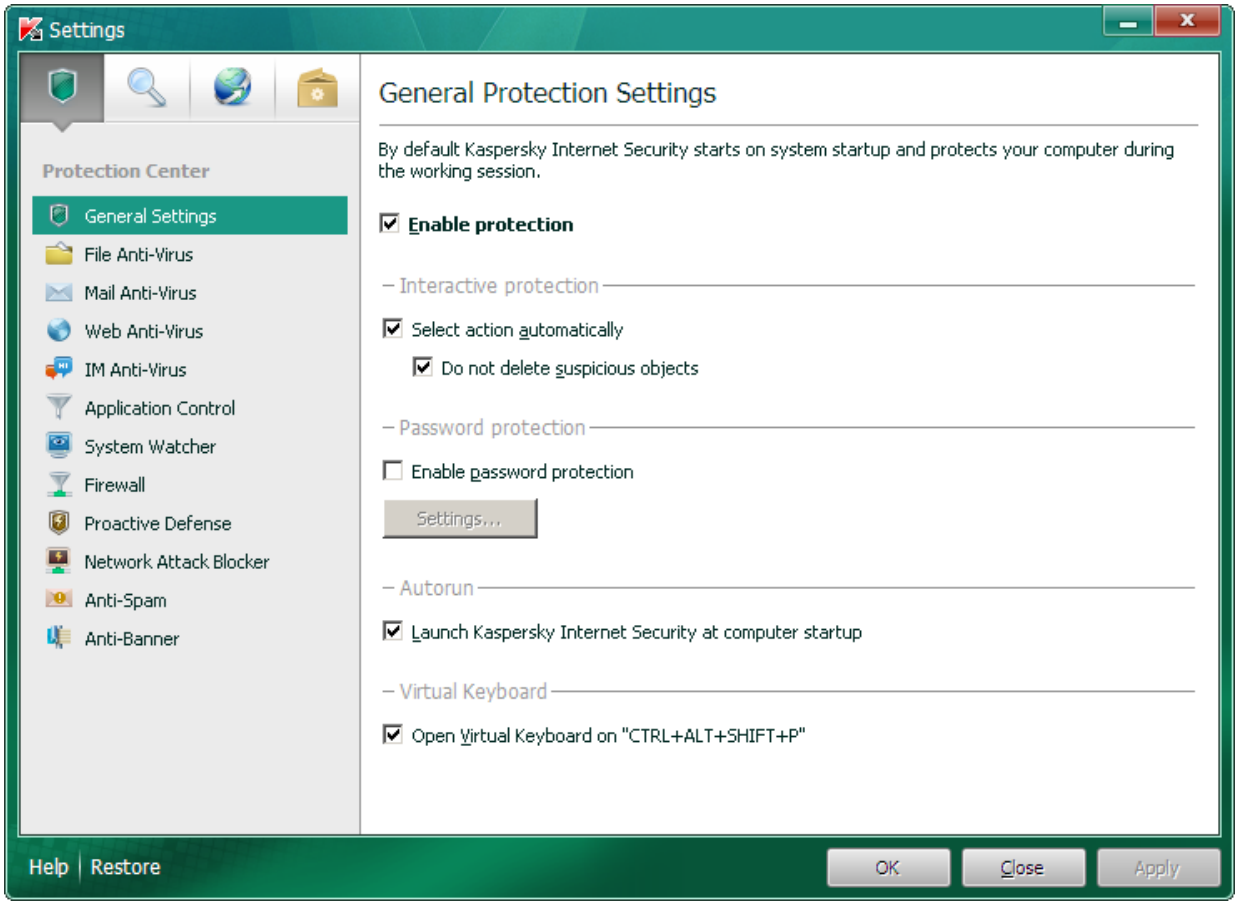


Figure 8. Application settings window

The application settings window consists of two parts:

- in the left part of the window you can choose the application component, task or another item that should be configured;
- the right part of the window contains the controls that you can use to configure the item selected in the left part of the window.

The components, tasks and other parts in the left part of the window are combined in the following sections:

– **Protection Center**;

– **Scan**;

– **Update Center**;

– **Advanced Settings**.

To open the settings window, perform one of the following actions:

- click the **Settings** link in the top part of the main application window (see section "Kaspersky Internet Security main window" on page 44);
- select **Settings** from the context menu (see section "Context menu" on page 43);
- click the button with the **Settings** icon in the Kaspersky Gadget interface (only for Microsoft Windows Vista and Microsoft Windows 7 operating systems). The option of option of opening the settings window should be assigned to the button (see section "How to use Kaspersky Gadget" on page 72).

To select the required section in the configuration window,

click the icon corresponding to the section in the top left part of the window (see the figure above).

KASPERSKY GADGET

When using Kaspersky Internet Security on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can also use the Kaspersky Gadget (hereinafter *gadget*).

Kaspersky Gadget is designed for quick access to the main features of the application: protection status indication, virus scan of objects, application operation reports, etc.

After you install Kaspersky Internet Security on a computer running under Microsoft Windows 7, the gadget appears on your desktop automatically. After you install the application on a computer running under Microsoft Windows Vista, you should add the gadget to Microsoft Windows Sidebar manually (see the operating system documentation).

Figure 9. Kaspersky Gadget

STARTING AND STOPPING THE APPLICATION

After Kaspersky Internet Security has been installed, it starts automatically. The application is launched automatically each time the operating system starts.

IN THIS SECTION:

Enabling and disabling automatic launch 50

Starting and stopping the application manually 50

ENABLING AND DISABLING AUTOMATIC LAUNCH

Automatic launch of the application means that Kaspersky Internet Security launches after the operating system startup. This is the default start mode.

- *To disable or enable automatic launch of the application:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **General Settings** subsection.
  3. To disable automatic launch of the application, uncheck the **Launch Kaspersky Internet Security at computer startup** box in the **Autorun** section, in the right part of the window. Check this box, to enable automatic launch of the application.

STARTING AND STOPPING THE APPLICATION MANUALLY

Kaspersky Lab specialists do not recommend that you stop Kaspersky Internet Security, because protection of your computer and personal data will be at risk. If disabling protection is really necessary, you are advised to pause your computer's protection for a specified period without exiting the application.

Kaspersky Internet Security should be started manually if you have disabled automatic launch of the application (see section "Enabling and disabling automatic launch" on page 50).

- *To launch the application manually,*

  in the **Start** menu, select **Programs** → **Kaspersky Internet Security 2011** → **Kaspersky Internet Security 2011**.

- *To exit the application,*

  right-click to open the context menu of the application icon in the taskbar notification area and select **Exit**.

In the Microsoft Windows 7 operating system the application icon is hidden by default, but you can display it to access the application more easily (see the operating system documentation).

COMPUTER PROTECTION STATUS

This section contains information about how to find out whether your computer is currently protected, or if its security is under threat, as well as how to eliminate emerging threats. In this section, you can also find information about enabling, disabling, and pausing protection when working with Kaspersky Internet Security.

IN THIS SECTION:

Diagnostics and elimination of problems in your computer protection 51

Enabling and disabling protection 53

Pausing and resuming protection 54

DIAGNOSTICS AND ELIMINATION OF PROBLEMS IN YOUR COMPUTER PROTECTION

Problems with computer protection are indicated by the computer protection status indicator located in the top part of the main application window (see section "Kaspersky Internet Security main window" on page 44). The indicator changes color depending upon the host protection status: green means that the computer is protected, yellow indicates protection-related problems, red alerts of serious threats to computer security. You are advised to fix the problems and security threats immediately.

Clicking the indicator icon in the main application window opens the **Protection state** window (see the figure below) containing detailed information about the status of computer protection and troubleshooting suggestions for the detected problems and threats.

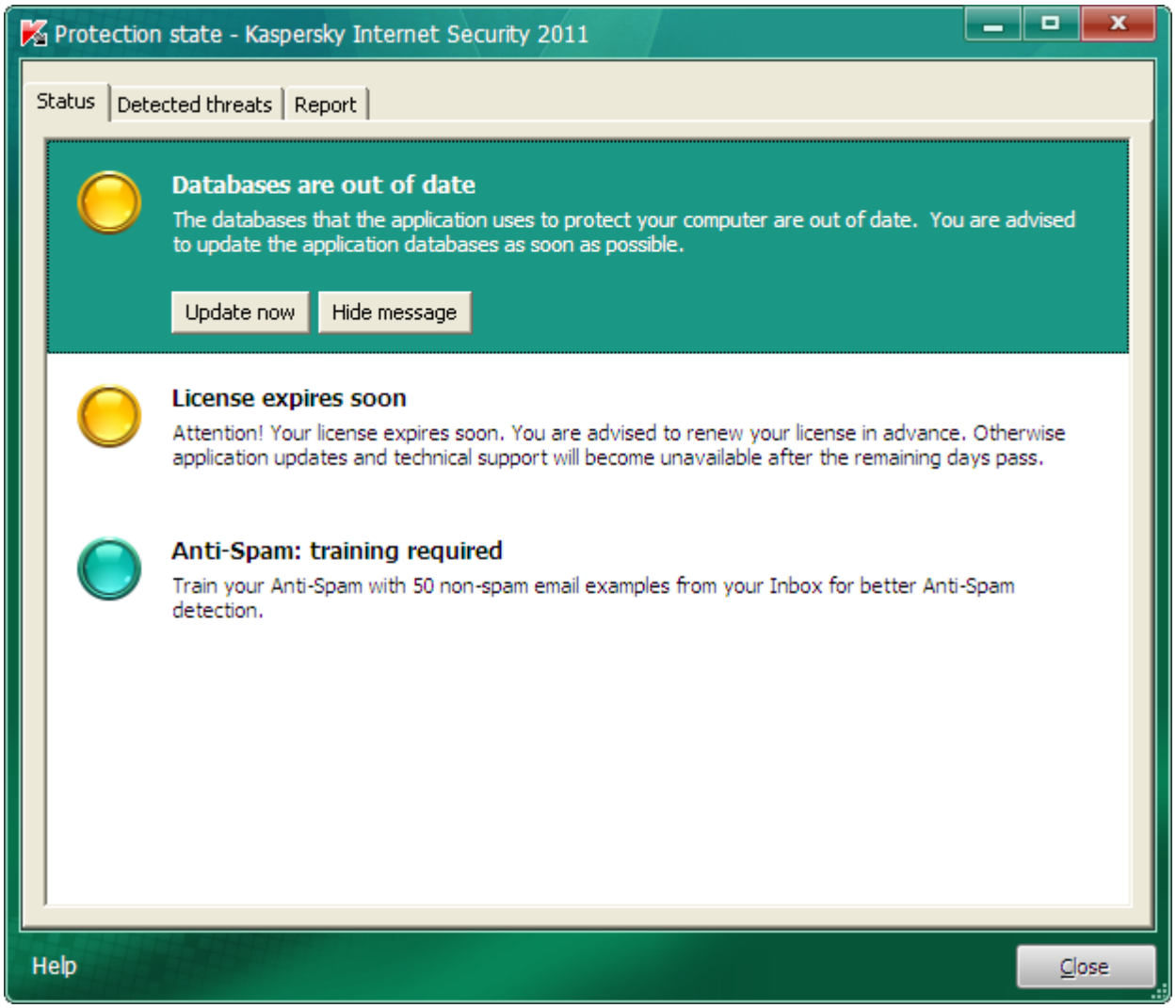

Protection state - Kaspersky Internet Security 2011
Status
Detected threats
Report
Databases are out of date
The databases that the application uses to protect your computer are out of date. You are advised to update the application databases as soon as possible.
Update now
Hide message
License expires soon
Attention! Your license expires soon. You are advised to renew your license in advance. Otherwise application updates and technical support will become unavailable after the remaining days pass.
Anti-Spam: training required
Train your Anti-Spam with 50 non-spam email examples from your Inbox for better Anti-Spam detection.
Help
Close

Figure 10. Resolving security problems

The **Status** tab of the **Protection state** window lists the protection-related problems including those caused by deviations from the normal product operation mode (e.g., outdated databases). To address the issues, the product offers the following options as further steps:

- Remove immediately. Clicking the corresponding buttons will take you to the appropriate problem solution. This is the recommended action.

- Postpone removal. If, for whatever reason, immediate removal of the problem is not possible, you can postpone this action and return to it later. To do this, click the **Hide message** button.

  Note that postponing the removal is not available for serious problems. Such problems include, for example, malicious objects that were not disinfected, crashes of one or several components, or corruption of program files.

To display the notifications hidden earlier in the common list, check the **Show hidden messages** box, which appears in the bottom part of the tab when there are hidden messages.

You can use the **Detected threats** tab to view the list of revealed malware and riskware and select the operation which will be performed over the objects (e.g., move to Quarantine). To select an operation, use the controls above the list and the context menu for the listed records.

On the **Report** tab, you can view the application activity reports (see section "Where to view the report on the application's operation" on page 70).

ENABLING AND DISABLING PROTECTION

By default, Kaspersky Internet Security is launched when the operating system loads and protects your computer until it is switched off. All protection components are running.

You can fully or partially disable the protection provided by Kaspersky Internet Security.

Kaspersky Lab specialists strongly recommend that you do not disable protection, since this may lead to an infection of your computer and data loss. If it is really necessary, we recommend that you pause protection for the required period of time (see section "Pausing and resuming protection" on page 54).

When protection is disabled, all its components become inactive.

This is indicated as follows:

- inactive (gray) application icon in the taskbar notification area (see section "Notification area icon" on page 42);
- red security indicator in the upper part of the main application window.

In this case, protection is seen in the context of the protection components. Disabling or pausing protection components does not effect the performance of virus scan tasks and Kaspersky Internet Security updates.

You can completely enable or disable protection in the application settings window (see section "Application settings window" on page 48). You can enable or disable separate application components either in the settings window, or in the main application window (see section "Kaspersky Internet Security main window" on page 44).

To completely enable or disable protection:

1. Open the application settings window.
2. In the left part of the window, select the **Protection Center** section, **General Settings** subsection.
3. Uncheck the **Enable protection** box if you need to disable protection. Check this box if you need to enable protection.

To enable or disable a protection component in the settings window:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the component that should be enabled or disabled.
3. In the right part of the window, uncheck the **Enable <component name>** box if you need to disable this component. Check this box if you need to enable the component.

To enable or disable a protection component in the main application window:

1. Open the main application window and select the **Protection Center** section.
2. In the right part of the window, left-click the section that comprises the component being enabled or disabled.
3. Open the action selection menu by clicking the button with the name of the component. Select **Enable <Component name>** if you need to enable this component, or select **Disable <Component name>** if you need to disable it.

   When enabling a component, the icon on its left turns green and when disabling it, the icon turns grey.

PAUSING AND RESUMING PROTECTION

Pausing protection means temporarily disabling all protection components for a certain period of time.

This is indicated as follows:

- inactive (gray) application icon in the taskbar notification area (see section "Notification area icon" on page 42);
- red security indicator in the upper part of the main application window.

In this case, protection is seen in the context of the protection components. Disabling or pausing protection components does not effect the performance of virus scan tasks and Kaspersky Internet Security updates.

If network connections were established at the same time as protection was paused, a notification about termination of such connections is displayed.

When working on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can pause protection using Kaspersky Gadget. To do this, Kaspersky Gadget should be configured so that the option of opening the reports window would be assigned to one of its buttons (see section "How to use Kaspersky Gadget" on page 72).

To pause the protection of your computer:

1. Open the **Pause protection** window using one of the following methods:
   - select **Pause protection** from the context menu of the application icon (see section "Context menu" on page 43);
   - click the button with the **Pause protection** icon in the Kaspersky Gadget interface (only for Microsoft Windows Vista and Microsoft Windows 7 operating systems).
2. In the **Pause protection** window, select the time interval after which the protection should be resumed:
   - **Pause for the specified time** – protection will be enabled after the time interval specified in the field below.
   - **Pause until reboot** – protection will be enabled after the application is restarted or the operating system is rebooted (provided that the automatic application launch is enabled (see section "Enabling and disabling automatic launch" on page 50)).
   - **Pause** – protection will only be enabled when you decide to resume it (please see below).

To resume computer protection,

select **Resume protection** from the context menu of the application icon (see section "Context menu" on page 43).

You can use this method to resume computer protection when the **Pause** option has been selected, or when you have selected **Pause for the specified time** or **Pause until reboot**.

SOLVING TYPICAL TASKS

This section contains instructions on the basic tasks encountered by most users when working with the application.

IN THIS SECTION:

How to activate the application 55

How to purchase or renew a license 56

What to do when the application's notifications appear 57

How to update application databases and modules 57

How to scan critical areas of your computer for viruses 58

How to scan a file, folder, disk, or another object for viruses 59

How to perform full scan of your computer for viruses 60

Scanning computer for vulnerabilities 61

How to protect your personal data against theft 61

What to do if you suspect an object of being infected with a virus 63

What to do with a large number of spam messages 64

What to do if you suspect your computer of being infected 65

How to restore an object that has been deleted or disinfected by the application 67

How to create and use Rescue Disk 67

How to view the report on the application's operation 70

How to restore application default settings 70

Transferring Kaspersky Internet Security settings to the product installed on another computer 71

How to use Kaspersky Gadget 72

HOW TO ACTIVATE THE APPLICATION

Activation is the procedure of activating a license that allows you to use a fully functional version of the application until the license expires.

If you have not activated the application during installation, you can do so later. You will be reminded about the need to activate the application by Kaspersky Internet Security messages appearing in the taskbar notification area.

➧ *To run the Kaspersky Internet Security activation wizard, perform one of the following:*

- Click the **Please activate the application** link in the Kaspersky Internet Security notice window appearing in the system tray.

- Click the **License** link in the bottom part of the main application window. In the **License management** window that opens, click the **Activate the application with a new license** button.

Let us review the steps of the Wizard in more detail.

Step 1. Selection of the license type and entry of the activation code

Make sure you have selected **Activate commercial license** in the Activation Wizard window, enter the activation code (see section "About activation code" on page 40) in the corresponding field, and click the **Next** button.

Step 2. Requesting for activation

At the first step, the Wizard sends a request to the activation server to obtain permission for activation of the commercial version of the application. If the request is sent successfully, the Wizard automatically proceeds to the next step.

Step 3. Entry of registration data

User registration is necessary for the user to be able to contact the Support Service. Unregistered users only receive minimal support.

Specify your registration data and click the **Next** button.

Step 4. Activation

At this step, the Wizard connects with the activation server in order to finish the application activation and user registration after which the Wizard automatically proceeds to the next window.

Step 5. Wizard completion

This window displays information on the activation results: type of license used and license expiry date.

Click the **Finish** button to close the Wizard.

HOW TO PURCHASE OR RENEW A LICENSE

If you have installed Kaspersky Internet Security without a license, you can purchase one after installation. When your license expires, you can renew it. You will receive an activation code that you should use to activate the application (see section "How to activate the application" on page 55).

To purchase a license:

1. Open the main application window.
2. Click the **Purchase license** button in the bottom part of the window.

   The eStore web page opens where you can purchase a license.

To renew a license:

1. Open the main application window and click the **License** link in the bottom part of the main window.

   The **License management** window opens.
2. Click the **Renew license** button.

   The license renewal center web page opens where you can renew your license.

WHAT TO DO WHEN THE APPLICATION'S NOTIFICATIONS APPEAR

Notifications that appear in the taskbar notification area inform you of events occurring in the application's operation and requiring your attention. Depending on how critical the event is, you may receive the following types of notification:

- Critical notifications – inform you of events of critical importance from the viewpoint of computer security: for example, detection of a malicious object or dangerous activity in the system. Notification windows and pop-up messages of this type are red-colored.
- Important notifications – inform you of events which are potentially important from the viewpoint of computer security: for example, detection of a potentially infected object or suspicious activity in the system. Notification windows and pop-up messages of this type are yellow-colored.
- Information notifications – inform you of events that are non-critical from the viewpoint of security. Notification windows and pop-up messages of this type are green-colored.

If such a notification is displayed on the screen, you should select one of the suggested options. By default, the optimum option is the one recommended by Kaspersky Lab experts.

HOW TO UPDATE APPLICATION DATABASES AND MODULES

By default, Kaspersky Internet Security automatically checks for updates on the Kaspersky Lab update servers. If the server contains new updates, the application downloads and installs them in the background mode. You can start a Kaspersky Internet Security update at any time.

To download updates from Kaspersky Lab servers, you should have an established Internet connection.

To start update from the context menu,

select **Update** from the context menu of the application icon.

To start update from the main application window:

1. Open the main application window and select the **Update Center** section in the left part of the window.
2. Click the **Run Update** button in the right part of the window.

   Information about the update in progress is displayed:

   - in the **Update** section of the main application window, in the **Update is in progress** subsection;
   - in the **Update** window, which opens when clicking the **Update is in progress** button;
   - in the context menu of the application icon.

To stop update:

1. Open the main application window and select the **Update Center** section in the left part of the window.
2. Click the **Update is in progress** button in the right part of the window.
3. In the **Update** window that opens, click the **Stop** button.
4. In the window that prompts the user for confirmation, click the **Yes** button.

HOW TO SCAN CRITICAL AREAS OF YOUR COMPUTER FOR VIRUSES

Scan of critical areas consists of scanning the objects which are loaded at startup of the operating system, scanning the system memory, boot sectors of the disk drive, and the objects that have been added by the user (see section "Creating a list of objects to scan" on page 80).

You can start the scan of critical areas using one of the following methods:

- using the shortcut created earlier (see page 84);
- from the main application window (see section "Kaspersky Internet Security main window" on page 44).

To start the scan using a shortcut:

1. Open Microsoft Windows Explorer and go to the folder where you have created the shortcut.
2. Double-click the shortcut to start the scan.

   Information about the scan in progress is displayed:

   - in the **Scan** section of the main application window, in the **Critical Areas Scan is in progress** section;
   - in the **Critical Areas Scan** window that opens by clicking the **Critical Areas Scan is in progress** button;
   - in the context menu of the application icon.

To start a scan from the main application window:

1. Open the main application window and select the **Scan** section in the left part of the window.
2. In the right part of the main application window, click the **Run Critical Areas Scan** button.

   Information about the scan in progress is displayed:

   - in the **Scan** section of the main application window, in the **Critical Areas Scan is in progress** section;
   - in the **Critical Areas Scan** window that opens by clicking the **Critical Areas Scan is in progress** button;
   - in the context menu of the application icon.

To stop the critical areas scan:

1. Open the main application window and select the **Scan** section in the left part of the window.
2. In the right part of the window, click the **Critical Areas Scan is in progress** button.
3. In the **Critical Areas Scan** window that opens, click the **Stop** button.
4. In the window that prompts the user for confirmation, click the **Yes** button.

HOW TO SCAN A FILE, FOLDER, DISK, OR ANOTHER OBJECT FOR VIRUSES

You can use the following methods to scan an object for viruses:

- using the context menu of the object;
- from the main application window (see section "Kaspersky Internet Security main window" on page 44);
- using the Kaspersky Internet Security Gadget (only for Microsoft Windows Vista and Microsoft Windows 7 operating systems).

To start a virus scan task from the object context menu:

1. Open Microsoft Windows Explorer and go to the folder which contains the object to be scanned.
2. Right-click to open the context menu of the object (see figure below) and select **Scan for Viruses**.

   The process and the results of the task will be displayed in the **Virus Scan** window that opens.

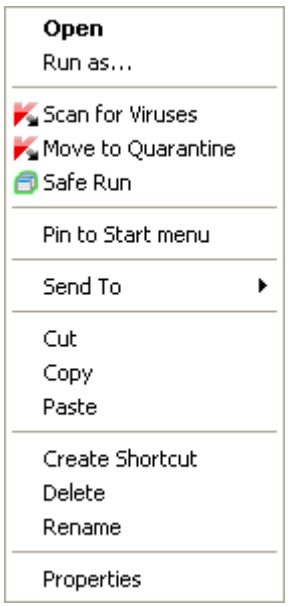


Figure 11. Context menu of an object in Microsoft Windows

To start scanning an object from the main application window:

1. Open the main application window and select the **Scan** section in the left part of the window.
2. Specify the object to scan, using one of the following methods:
   - Click the **select** link in the right part of the window to open the **Custom Scan** window, and check the boxes next to the folders and drives that you need to scan. If the window displays no objects to scan, open the **Select object to scan** window by clicking the **Add** link, and select objects to scan.
   - Drag an object to scan into the dedicated area of the main window (see figure below).

Task progress is displayed in the **Virus Scan** window that opens.

Figure 12. Window area into which you should drag an object to scan

- *To scan an object for viruses using the gadget,*

  drag the object to scan onto the gadget.

  Task progress is displayed in the **Virus Scan** window that opens.

- *To stop objects scan:*

  1. In the **Virus Scan** window that opens after the objects scan starts, click the **Stop** button, or close the window.
  2. In the Virus Scan window that opens, prompting the user for confirmation of scan stop, click the **Yes** button.

HOW TO PERFORM FULL SCAN OF YOUR COMPUTER FOR VIRUSES

You can start a full scan for viruses using one of the following methods:

- using the shortcut created earlier (see page 84);
- from the main application window (see section "Kaspersky Internet Security main window" on page 44).

- *To start the full scan using a shortcut:*

  1. Open the Microsoft Windows Explorer window and go to the folder where you have created the shortcut.
  2. Double-click the shortcut to start the scan.

     Information about the scan in progress is displayed:

     - in the **Scan** section of the main application window, in the **Full Scan is in progress** section;
     - in the **Full Scan** window that opens by clicking the **Full Scan is in progress** section;
     - in the context menu of the application icon.

- *To start a full scan from the main application window:*

  1. Open the main application window and select the **Scan** section in the left part of the window.
  2. In the right part of the window, click the **Run Full Scan** button.

     Information about the scan in progress is displayed:

     - in the **Scan** section of the main application window, in the **Full Scan is in progress** section;
     - in the **Full Scan** window that opens by clicking the **Full Scan is in progress** section;
     - in the context menu of the application icon.

To stop the full scan:

1. Open the main application window and in the left part of it select the section named **Scan**.
2. In the right part of the window, click the **Full Scan is in progress** button.
3. In the **Full Scan** window that opens, click the **Stop** button.
4. In the window that prompts the user for confirmation, click the **Yes** button.

SCANNING COMPUTER FOR VULNERABILITIES

Vulnerabilities are unprotected portions of software code which intruders may deliberately use for their purposes, for example, to copy data used in unprotected applications. Scanning your computer for vulnerabilities helps you to reveal any such weak points in your computer. You are advised to remove the detected vulnerabilities.

You can use the following methods to scan the system for vulnerabilities:

- from the main application window (see section "Kaspersky Internet Security main window" on page 44);
- using the shortcut created earlier.

To start the task using a shortcut:

1. Open the Microsoft Windows Explorer window and go to the folder where you have created the shortcut.
2. Double-click the shortcut to start scanning the system for vulnerabilities.

   Progress of the task will be displayed in the **Vulnerability Scan** window that opens.

To start the task from the main application window:

1. Open the main application window and select the **Tools** section in the left part of the window.
2. Click the **Vulnerability Scan** button in the right part of the window.

   Progress of the task will be displayed in the **Vulnerability Scan** window that opens.

To stop the vulnerability scan:

1. Open the main application window and select the **Tools** section in the left part of the window.
2. Click the **Vulnerability Scan** button in the right part of the window.
3. In the **Vulnerability Scan** window that opens, click the **Stop** button.
4. In the window that prompts the user for confirmation of the scan stop, click the **Yes** button.

HOW TO PROTECT YOUR PERSONAL DATA AGAINST THEFT

With Kaspersky Internet Security, you can protect your personal data against theft; this includes items such as:

- passwords, usernames, and other registration data;
- account numbers and bank cards.

Kaspersky Internet Security includes components and tools that allow you to protect your personal data against theft attempts committed by hackers using methods such as phishing and the interception of data entered via the keyboard.

Protection against phishing is ensured by Anti-Phishing implemented in the Web Anti-Virus, Anti-Spam, and IM Anti-Virus components.

Protection against the interception of data entered at the keyboard is ensured by the use of *Virtual Keyboard*.

IN THIS SECTION:

Protection against phishing 62

Virtual Keyboard..... 62

PROTECTION AGAINST PHISHING

Phishing is a type of online fraud that involves tricking users into disclosing their credit card numbers, PIN codes and other personal details with the objective of stealing funds.

Phishing often targets online banking users. Criminals create an exact copy of the website of a chosen bank and send emails to customers on behalf of this bank. They claim that a malfunction or replacement of online banking system software has resulted in the loss of user details, necessitating the user to confirm or modify such details on the bank's website. Users click the link that takes them to the fake website and enter their details, which then end up in the hands of criminals.

Protection against phishing is ensured by Anti-Phishing implemented in the Web Anti-Virus, Anti-Spam, and IM Anti-Virus components. Enable these components to ensure comprehensive protection against phishing.

To enable components providing protection against phishing:

1. Open the main application window and select the **Protection Center** section in the left part of the window.
2. In the right part of the window, left-click to open the **Online Security** section.
3. Open the menu for selecting an action on the component by clicking the **Anti-Phishing** button and select **Enable Anti-Phishing** item from the menu.

   This action enables Anti-Phishing and all components that it makes part of.

VIRTUAL KEYBOARD

When working on your computer, there are occasions when entering of your personal data, or username and password are required. That happens, for example, during account registration on web sites, web shopping or Internet banking.

There is a risk that this personal information is intercepted using hardware keyboard interceptors or keyloggers, which are programs that register keystrokes.

The Virtual Keyboard tool prevents the interception of data entered via the keyboard.

The Virtual Keyboard cannot protect your personal data if the website requiring the entry of such data has been hacked, because in this case the information is obtained directly by the intruders.

Many of the applications classified as spyware have the function of making screenshots which are then transferred to an intruder for further analysis and for stealing the user's personal data. Virtual Keyboard prevents the personal data being entered from being intercepted with the use of screenshots.

The Virtual Keyboard only prevents the interception of privacy data when working with Microsoft Internet Explorer and Mozilla Firefox browsers.

Before you start using the Virtual Keyboard, please learn its peculiarities:

- Before entering data from the Virtual Keyboard, using the cursor, make sure that the appropriate entry field is selected.
- You can click the Virtual Keyboard buttons using the mouse.
- Unlike real keyboards, there is no way of clicking two keys simultaneously on a Virtual Keyboard. Therefore, to use combinations of keys (e.g., **ALT+F4**), you have to click the first key (e.g., **ALT**), then the next key (e.g., **F4**), and then click the first key again. The second click of the key acts in the same way as the key release on a real keyboard.
- Input language for the Virtual Keyboard is toggled using the **CTRL+SHIFT** key combination (the **SHIFT** key should be clicked using the right mouse button) or **CTRL+LEFT ALT** (the **LEFT ALT** key should be clicked using the right mouse button) depending upon the specified settings.

You can open the Virtual Keyboard in the following ways:

- from the context menu of the application icon;
- from the main application window;
- from the Microsoft Internet Explorer or Mozilla Firefox browser windows;
- using the keyboard shortcuts.

To open the Virtual Keyboard from the context menu of the application icon,

select **Tools** → **Virtual Keyboard** from the context menu of the application icon.

To open the Virtual Keyboard from the main application window,

in the **Safe Run** section of the main application window, click the **Virtual Keyboard** button.

To open the Virtual Keyboard from the browser window,

click the **Virtual Keyboard** button in the toolbar of Microsoft Internet Explorer or Mozilla Firefox.

To open the Virtual Keyboard using the computer keyboard,

press the **CTRL+ALT+SHIFT+P** shortcut.

WHAT TO DO IF YOU SUSPECT AN OBJECT OF BEING INFECTED WITH A VIRUS

If you suspect an object of being infected, first scan it using Kaspersky Internet Security (see section "How to scan a file, folder, disk, or another object for viruses" on page 59).

After the scan, if the application reports that the object is not infected, but you think that it is, you can do the following:

- Move the object to *Quarantine*. Objects moved to Quarantine do not pose any threat to your computer. After the databases are updated, Kaspersky Internet Security will probably be able to clearly identify and remove the threat.
- Send the object to *Virus Lab*. Virus Lab specialists scan the object. If it turns out to be infected with a virus, they immediately add the description of the new virus in the databases that will be downloaded by the application with an update (see section "How to update application databases and modules" on page 57).

You can move an object to Quarantine using one of the two methods:

- using the **Move to Quarantine** link in the **Protection state** window;
- using the context menu of the object.

To move an object to Quarantine from the Protection state window:

1. Open the main application window.
2. Click the **Quarantine** link in the top part of the main window to open the **Protection state** window on the **Detected threats** tab.
3. Click the **Move to Quarantine** button.
4. In the window that opens, select the object that you want to move to Quarantine.

To move an object to Quarantine using the context menu:

1. Open Microsoft Windows Explorer and go to the folder with the object that should be moved to Quarantine.
2. Right-click to open the context menu of the object and select **Move to Quarantine**.

To send an object to the Virus Lab:

1. Go to the Virus Lab request page (http://support.kaspersky.com/virlab/helpdesk.html).
2. Follow the instructions on this page to send your request.

WHAT TO DO WITH A LARGE NUMBER OF SPAM MESSAGES

If you receive large quantities of unsolicited mail (spam), enable the Anti-Spam component and set the recommended security level. Then train the component using the *Training Wizard*. Correct spam recognition requires training using at least 50 samples of useful messages and 50 samples of unwanted mail.

To enable Anti-Spam and set the recommended security level:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. In the right part of the window, check the **Enable Anti-Spam** box.
4. In the **Security level** section, the security level should be set to **Recommended** by default.

   If the security level is set to **Low** or **Custom**, click the **Default level** button. The security level will automatically be set to **Recommended**.

To train Anti-Spam using the Training Wizard:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Train** button in the **Anti-Spam training** section within the right part of the window.

   The Training Wizard window will open.

The Wizard steps in detail.

Step 1. Starting the Wizard

Click the **Next** button to start the training.

Step 2. Selecting folders containing good mail

At this stage, you can specify folders which contain good mail. You should only select folders which you are absolutely sure contain good email messages.

Only Microsoft Office Outlook and Microsoft Outlook Express (Windows Mail) accounts are accessible.

Step 3. Selecting folders containing spam

At this stage you can specify folders containing unsolicited mail (spam). If you do not have such folders in your email client application, skip this step.

Only Microsoft Office Outlook and Microsoft Outlook Express (Windows Mail) accounts are accessible.

Step 4. Training Anti-Spam

At this stage, the Anti-Spam component is trained using the folders selected during the previous steps. The emails in those folders fill the Anti-Spam database. The senders of good mail are automatically added to the list of allowed senders.

Step 5. Saving the training results

At this stage of the Wizard, you must save the training results using one of the following methods:

- add training results into the existing Anti-Spam database (select **Add the results to an existing Anti-Spam database**);
- replace the current database with a database containing only the training results (select the option **Create new Anti-Spam database**).

Click the **Finish** button to close the Wizard.

WHAT TO DO IF YOU SUSPECT YOUR COMPUTER OF BEING INFECTED

If you suspect that your computer has been infected, use the *System Restore Wizard* to neutralize the consequences of malicious activity in the system. Kaspersky Lab recommends that you run the Wizard after the computer has been disinfected to make sure that all threats and damage caused by infections have been fixed.

The Wizard checks whether there are any changes to the system, such as the following: access to the network being blocked, known file format extensions have been changed, the toolbar is locked, etc. Such damage can have various causes. The latter may include the activity of malicious programs, incorrect system configuration, system failures or even incorrect operation of system optimization applications.

After the review is complete, the Wizard analyzes the information to evaluate whether there is system damage which requires immediate attention. Based on the review, a list of actions necessary to eliminate the problems is generated. The Wizard groups these actions by category based on the severity of the problems detected.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

To start the System Restore Wizard:

1. Open the main application window and select the **Tools** section in the left part of the window.
2. In the right part of the window click the **System Restore** button.

The Wizard steps in detail.

Step 1. Starting system restore

Make sure that the Wizard option to **Search for problems caused by malware activity** is selected and click the **Next** button.

Step 2. Problem search

The Wizard will search for problems and damage, which should be fixed. Once the search is complete, the Wizard will automatically proceed to the next step.

Step 3. Selecting troubleshooting actions

All damage found during the previous step is grouped on the basis of the type of danger it poses. For each damage group, Kaspersky Lab recommends a sequence of actions to repair the damage. There are three groups of actions:

- *Strongly recommended actions* eliminate problems posing a serious security threat. You are advised to perform all actions in this group.
- *Recommended actions* eliminate problems presenting a potential threat. You are also advised to perform all actions in this group.
- *Additional actions* repair system damage which does not pose a current threat, but may pose a danger to the computer's security in the future.

To view the actions within a group, click the **+** icon to the left of the group name.

To make the Wizard perform a certain action, check the box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, uncheck the box next to it.

It is strongly recommended not to uncheck the boxes selected by default because doing so will leave your computer vulnerable to threats.

Having defined the set of actions, which the Wizard will perform, click the **Next** button.

Step 4. Problems elimination

The Wizard will perform the actions selected during the previous step. The elimination of problems may take some time. Once the troubleshooting is complete, the Wizard will automatically proceed to the next step.

Step 5. Wizard completion

Click the **Finish** button to close the Wizard.

HOW TO RESTORE AN OBJECT THAT HAS BEEN DELETED OR DISINFECTED BY THE APPLICATION

Kaspersky Lab recommends that you avoid restoring deleted and disinfected objects since they may pose a threat to your computer.

If you want to restore a deleted or disinfected object, you can use a backup copy of it which was created by the application when scanning the object.

To restore an object that has been deleted or disinfected by the application:

1. Open the main application window.
2. Click the **Quarantine** link in the top part of the main window to open the **Protection state** window on the **Detected threats** tab.
3. From the dropdown list located over the list of threats, select **Neutralized**.

   The list of disinfected and deleted objects is displayed on the **Detected threats** tab. Objects are grouped according to their status. To display the list of objects in a group, click the **+** icon located to the left of the group header.
4. Right-click to open the context menu of the object that you want to restore, and select **Restore**.

HOW TO CREATE AND USE RESCUE DISK

We recommend that you create Rescue Disk after you have installed and configured Kaspersky Internet Security, scanned your computer, and made sure that it was not infected. You will further be able to use Rescue Disk for scanning and disinfecting infected computers that cannot be disinfected using other methods (e.g., with anti-virus applications).

IN THIS SECTION:

Create Rescue Disk 67

Starting the computer from the Rescue Disk 69

CREATE RESCUE DISK

Creating the Rescue Disk means the creation of a disk image (ISO file) with up-to-date anti-virus databases and configuration files.

The source disk image serving as a base for new file creation can be downloaded from the Kaspersky Lab server or copied from a local source.

You can create Rescue Disk using the *Rescue Disk Creation Wizard*. The rescuecd.iso file created by the Wizard is saved on your computer's hard drive:

- in Microsoft Windows XP – in the following folder: Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Data\Rdisk\;
- in Microsoft Windows Vista and Microsoft Windows 7 operating systems – in the following folder: ProgramData\Kaspersky Lab\AVP11\Data\Rdisk\.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

To start the Rescue Disk Creation Wizard:

1. Open the main application window and select the **Tools** section in the left part of the window.
2. In the right part of the window click the **Rescue Disk** button.

The Wizard steps in detail.

Step 1. Starting the Wizard. Searching for an existing disk image

The first window of the Wizard contains information about the Rescue Disk that will be created by the Wizard.

If the Wizard detects an existing Rescue Disk ISO file in the dedicated folder (see above), the **Use existing ISO image** box will be displayed in the first window of the Wizard. Check the box to use the detected file as original ISO image and go directly to the **Updating disk image** step (see below). Uncheck this box if you do not want to use the disk image that has been found, and the Wizard proceeds to the **Select disk image source** window.

Step 2. Select disk image source

If you have checked the **Use existing ISO image** box in the first Wizard window, then this step will be skipped.

At this step, you should select the image file source from the list of options:

- Select **Copy ISO image from local or network drive** if you already have a Rescue Disk or an image prepared for it and stored on your computer or on a local network resource.
- Select the **Download ISO image from Kaspersky Lab server** option if you do not have an image file, and you want to download it from the Kaspersky Lab server (file size is about 100 MB).

Step 3. Copying (downloading) disk image

If you have checked the **Use existing ISO image** box in the first Wizard window, then this step will be skipped.

If you have selected the option to copy the image from a local source at the previous step (**Copy ISO image from local or network drive**), you should specify the path to the ISO file at this current step. To do this, click the **Browse** button. After you have specified the path to the file, click the **Next** button. The disk image copying progress is displayed in the Wizard window.

If you have selected **Download ISO image from Kaspersky Lab server**, the disk image downloading progress is displayed immediately.

When copying or downloading the ISO image is complete, the Wizard automatically proceeds to the next step.

Step 4. Updating image file

File update procedure includes:

- update of anti-virus databases;
- update of configuration files.

Configuration files determine the possibility of starting the computer from a removable disk or CD / DVD written using a rescue disk image provided by the Wizard.

When updating anti-virus databases, those distributed at the last update of Kaspersky Internet Security are used. If the databases are obsolete, it is recommended to update and restart the Rescue Disk Creation Wizard.

To begin updating the ISO file, click the **Next** button. The updating progress will be displayed in the Wizard window.

Step 5. Recording the image on a data medium

In this window, the Wizard informs you of a successful creation of the Rescue Disk and offers you to record it on a data medium.

Specify a data medium for recording the ISO image:

- Select **Record to CD / DVD** to record the image on a CD / DVD.

  You will be prompted to specify the CD / DVD on which the image should be recorded. Then, the ISO image will be recorded on this CD / DVD. The recording process may take some time so please wait until it has completed.

- Select the **Record to USB flash drive** option to record the image on a removable drive.

  Kaspersky Lab recommends that you do not record the ISO image on devices which are not designed specifically for data storage, such as smartphones, cellphones, PDAs, and MP3 players. Recording ISO images on these devices may lead to their incorrect functioning in the future.

  You will be prompted to specify the removable drive on which the image should be recorded. Then, the image will be recorded on this removable drive. The recording process may take some time so please wait until it has completed.

- Select **Save the disk image to file on local or network drive** to record the ISO image to the hard drive installed on your computer or another one that you can access over a network.

  You will be offered to specify the folder into which the image should be recorded, and the name of the ISO file, after which it will be recorded on the hard drive. The recording process may take some time so please wait until it has completed.

Step 6. Wizard completion

To complete the Wizard, click the **Finish** button. You can use the disk that you have created for further booting of the computer (see page 69).

STARTING THE COMPUTER FROM THE RESCUE DISK

If the operating system cannot be started as a result of a virus attack, use the Rescue Disk.

To boot the operating system, you should use a CD / DVD or removable drive with the rescue disk image (.iso) file recorded on it (see section "Creating the Rescue Disk" on page 67).

Loading a computer from a removable drive is not always possible. In particular, this mode is not supported by some obsolete computer models. Before shutting down your computer for further booting from a removable drive, make sure that this operation can be performed.

➧ *To boot your computer from the Rescue Disk:*

1. In the BIOS settings, enable booting from a CD / DVD or removable drive (for detailed information please refer to the documentation for your computer's motherboard).

2. Insert a CD / DVD with the Rescue Disk image into the CD/DVD drive of an infected computer or connect a removable drive to it.

3. Restart your computer.

For detailed information about the use of the Rescue Disk, please refer to the Kaspersky Rescue Disk User Guide.

HOW TO VIEW THE REPORT ON THE APPLICATION'S OPERATION

Kaspersky Internet Security creates operation reports for each component. Using a report, you can find out, for example, how many malicious objects (such as viruses and Trojan programs) have been detected and removed by the application during the specified period, how many times the application has been updated during the same period, how many spam messages have been detected, and many other characteristics.

When working on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can open reports using Kaspersky Gadget. To do this, Kaspersky Gadget should be configured so that the option of opening the reports window would be assigned to one of its buttons (see section "How to use Kaspersky Gadget" on page 72).

To view the application operation report:

1. Open the **Protection state** window on the **Report** tab using one of the following methods:

   - click the **Reports** link in the top part of the main application window;

   - click the button with the **Reports** icon in the Kaspersky Gadget interface (only for Microsoft Windows Vista and Microsoft Windows 7).

   The **Report** tab displays application operation reports in diagram format.

2. If you want to view a detailed application operation report (for example, a report representing the operation of each component), click the **Detailed report** button in the bottom part of the **Report** tab.

   The **Detailed report** window opens where data are represented in a table. For a convenient view of reports, you can select various entry sorting options.

HOW TO RESTORE APPLICATION DEFAULT SETTINGS

You can always restore the Kaspersky Internet Security settings which are recommended by Kaspersky Lab and considered optimal. The settings can be restored using the *Application Configuration Wizard*.

When the Wizard completes its operations, the **Recommended** security level is set for all protection components. While restoring the settings, you will also be prompted to define which settings should or should not be kept for which components together with restoring the recommended security level.

To restore protection settings:

1. Open the application settings window.

2. Run the Application Configuration Wizard using one of the following methods:

   - click the **Restore** link in the bottom part of the window;

   - in the left part of the window, select the **Advanced Settings** section, **Manage Settings** subsection, and click the **Restore** button in the **Restore default settings** section.

The Wizard steps in detail.

Step 1. Starting the Wizard

Click the **Next** button to proceed with the Wizard.

Step 2. Selecting settings to save

This Wizard window shows which Kaspersky Internet Security components have settings that differ from the default value, either because they were changed by the user, or were changed because of accumulated training by Kaspersky Internet Security (Firewall or Anti-Spam). If special settings have been created for any of the components, they will also be shown in the window.

Special settings include the lists of allowed and blocked phrases and addresses used by Anti-Spam, lists of trusted web addresses and ISP phone numbers, exclusion rules created for application components, Firewall packet and application filtering rules.

These lists are created when working with Kaspersky Internet Security with regard to individual tasks and security requirements. Creating the lists is often time consuming, so you are advised to save them before restoring the application's default settings.

Check the boxes for the settings that you want to save and click the **Next** button.

Step 3. System analysis

At this stage, information about Microsoft Windows applications is collected. These applications are added to the list of trusted applications which have no restrictions imposed on the actions they perform in respect of the system.

Once the analysis is complete, the Wizard will automatically proceed to the next step.

Step 4. Finishing restoration

To complete the Wizard, click the **Finish** button.

TRANSFERRING KASPERSKY INTERNET SECURITY SETTINGS TO THE PRODUCT INSTALLED ON ANOTHER COMPUTER

Having configured the product, you can apply its settings in Kaspersky Internet Security installed on another computer. Consequently, the application will be configured identically on both computers. This is a helpful feature when, for example, Kaspersky Internet Security is installed on your home computer and in your office.

Application settings are stored in a special configuration file, which you can transfer to another computer. To do this:

1. Perform the *Export* procedure – save the application settings to a configuration file.
2. Move the file you have saved to another computer (for example, send it by email or use a removable data medium).
3. Perform the *Import* procedure – apply the settings from the configuration file to the application installed on another computer.

To export the current settings of Kaspersky Internet Security:

1. Open the application settings window.
2. Select the **Manage Settings** section in the left part of the window.
3. Click the **Save** button in the right part of the window.
4. In the window that opens enter the name of the configuration file and the path where it should be saved.

To import the application's settings from a saved configuration file:

1. Open the application settings window.
2. Select the **Manage Settings** section in the left part of the window.
3. Click the **Load** button in the right part of the window.
4. In the window that opens, select a file from which you wish to import the Kaspersky Internet Security settings.

HOW TO USE KASPERSKY GADGET

When using Kaspersky Internet Security on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can also use the Kaspersky Gadget (hereinafter *gadget*).

After you install Kaspersky Internet Security on a computer running under Microsoft Windows 7, the gadget appears on your desktop automatically. After you install the application on a computer running under Microsoft Windows Vista, you should add the gadget to Microsoft Windows Sidebar manually (see the operating system documentation).

The Gadget color indicator displays your computer protection status in the same manner as the protection status indicator in the main application window (see section "Kaspersky Internet Security main window" on page 44). Green indicates that your computer is duly protected, while yellow indicates that there are protection problems, and red indicates that your computer' security is at serious risk. The gray color indicates that the application is stopped.

The gadget's appearance allows you to monitor update downloads: when the updating of databases and application modules is in progress, a spinning globe icon appears in the center of the Gadget.

You can use the gadget to perform the following main tasks:

- run the application if it has been stopped;
- open the main application window;
- scan specified objects for viruses;
- open the news window.

To run the application using the gadget,

click the **Enable** icon located in the center of the gadget.

To open the main application window using the gadget,

click Kaspersky Internet Security located in the center of the gadget.

To scan an object for viruses using the gadget,

drag the object to scan onto the gadget.

Task progress is displayed in the **Virus Scan** window that opens.

To open the news window using the gadget,

click the icon which is displayed in the center of the gadget when a piece of news is released.

Configuring the gadget

You can configure gadget so that you can use its buttons to initiate the following actions:

- edit the application settings;
- view application reports;
- switch to the safe desktop (only for 32-bit operating systems);
- view Parental Control reports;
- view information about network activity (Network Monitor);
- pause protection.

Additionally, you can change the gadget's appearance by selecting another skin for it.

To configure the gadget:

1. Open the gadget settings window by clicking the icon that appears in the right top corner of the gadget block if you roll over it with the mouse cursor.
2. From the **Left icon** and **Right icon** dropdown lists, select the actions that should be performed when clicking the left and right buttons of the gadget.
3. Select a skin for the gadget by clicking the buttons.
4. Click the **OK** button to save the changes that you have made.

ADVANCED APPLICATION SETTINGS

This section provides detailed information about each application component and describes the operation and configuration algorithms for each component.

To adjust the advanced application settings, open the settings window using one of the following methods:

- click the **Settings** link in the top part of the main application window;
- select **Settings** from the context menu of the application icon.

IN THIS SECTION:

General protection settings 75
Scan 77
Update 84
File Anti-Virus 89
Mail Anti-Virus 95
Web Anti-Virus 100
IM Anti-Virus 107
Proactive Defense 109
System Watcher 111
Application Control 113
Network protection 121
Anti-Spam 132
Anti-Banner 148
Safe Run 151
Parental Control 156
Trusted zone 165
Performance and compatibility with other applications 167
Kaspersky Internet Security self-defense. 170
Quarantine and Backup 171
Additional tools for better protection of your computer 174
Reports 178
Application appearance 182
Notifications 184
Participating in the Kaspersky Security Network 185

GENERAL PROTECTION SETTINGS

In the application settings window, in the **General Settings** subsection of the **Protection Center** section, you can perform the following operations:

- disable all protection components (see section "Enabling and disabling protection" on page 53);
- select the interactive or automatic protection mode (see section "Selecting protection mode" on page 76);

- restrict users' access to the application by setting a password (see section "Restricting access to Kaspersky Internet Security" on page 76);
- disable or enable automatic launch of the application at the startup of the operating system (see section "Enabling and disabling automatic launch" on page 50);
- enable a custom key combination to display the virtual keyboard on the screen (see section "Virtual Keyboard" on page 62).

IN THIS SECTION:

Restricting access to Kaspersky Internet Security 76

Selecting protection mode 76

RESTRICTING ACCESS TO KASPERSKY INTERNET SECURITY.

A computer may be used by several users with various levels of computer literacy. Unrestricted access to Kaspersky Internet Security and its settings granted to users may lead to reduced level of computer protection.

To restrict access to the application, you can set a password and specify which actions should require entering the password:

- changing application settings;
- enabling and configuring Parental Control;
- closing the application;
- removing the application.

Use a password for restricting access to the application removal with care. If you forget the password, the application will be hard to remove from your computer.

To restrict access to Kaspersky Internet Security with a password:

1. Open the application settings window.
2. In the left part of the window, select the **Protection Center** section, **General Settings** subsection.
3. In the right part of the window, in the **Password protection** section, check the **Enable password protection** box and click the **Settings** button.
4. In the **Password protection** window that opens, enter the password and specify the area to be covered by the access restriction.

SELECTING PROTECTION MODE

By default, Kaspersky Internet Security runs in *automatic protection mode*. In this mode the application automatically applies actions recommended by Kaspersky Lab in response to dangerous events. If you wish Kaspersky Internet Security to notify you of all hazardous and suspicious events in the system and to allow to decide which of the actions offered by the application should be applied, you can enable *interactive protection mode*.

To select protection mode:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **General Settings** subsection.
3. In the **Interactive protection** section check or uncheck the boxes depending on the selected protection mode:
   - to enable interactive protection mode, uncheck the **Select action automatically**;
   - to enable automatic protection mode, check the **Select action automatically**.

     If you do not want Kaspersky Internet Security to delete suspicious objects when running in automatic mode, check the **Do not delete suspicious objects** box.

SCAN

Scanning the computer for viruses and vulnerabilities is one of the most important tasks in ensuring the computer's security. It is necessary to scan your computer for viruses on a regular basis in order to rule out the possibility of spreading malicious programs that have not been discovered by security components, for example, because the security level was set to low or for other reasons.

Vulnerability scan performs the diagnostics of operating system and detects software features that can be used by intruders to spread malicious objects and obtain access to personal information.

The following sections contain detailed information about scan tasks features and configuration, security levels, scan methods, and scan technologies.

IN THIS SECTION:

Virus scan 77

Vulnerability Scan 84

VIRUS SCAN

Kaspersky Internet Security comprises the following tasks to scan for viruses:

- **Custom Scan**. Scan of objects selected by the user. You can scan any object of the computer's file system from the following list: system memory, objects loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Full Scan**. A thorough scan of the entire system. The following objects are scanned by default: system memory, objects loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Critical Areas Scan**. Virus scan of operating system startup objects.

The Full Scan and the Critical Areas Scan tasks have their peculiarities. For these tasks, it is not recommended to edit the lists of objects to scan.

Each scan task is performed in the specified area and can be started according to the schedule created. Each scan task is characterized with a security level (combination of settings that impact the depth of the scan). By default, the mode of using records from application databases to search for threats is always enabled. You can also apply various scan methods and technologies (see page 81).

After you run the full scan task or critical areas scan task, the progress of task run is displayed in the **Scan** section of the Kaspersky Internet Security main window, in the field under the name of the task being run.

If a threat is detected, Kaspersky Internet Security assigns one of the following statuses to the found object:

- malicious program (such as a *virus* or *Trojan*);
- *potentially infected* (suspicious) status if the scan cannot determine whether the object is infected or not. The file may contain a sequence of code appropriate for viruses, or modified code from a known virus.

The application displays a notification about detected threat and performs the assigned action. You can change actions to be performed on detected threat.

If you work in automatic mode (see section "Selecting protection mode" on page 76), Kaspersky Internet Security will automatically apply the action recommended by Kaspersky Lab specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Move to Quarantine**.

Before attempting to disinfect or delete an infected object, Kaspersky Internet Security creates a backup copy for subsequent restoration or disinfection. Suspicious (potentially infected) objects are quarantined. You can enable the automatic scan of quarantined objects after each update.

Information on the scan results and events, which have occurred during the execution of the task, is logged in a Kaspersky Internet Security report.

SEE ALSO:

How to perform full scan of your computer for viruses

How to scan critical areas of your computer for viruses

How to scan a file, folder, disk, or another object for viruses

IN THIS SECTION:

Changing and restoring security level
Creating the scan startup schedule
Creating a list of objects to scan
Selecting the scan method
Selecting the scan technology
Changing actions to be performed on detected objects
Running scan under a different user account
Changing the type of objects to scan
Scan of compound files
Scan optimization
Scanning removable drives on connection
Creating a task shortcut

CHANGING AND RESTORING SECURITY LEVEL

Depending on your current needs, you can select one of the preset security levels, or modify the scan settings manually.

When configuring scan task settings, you can always restore the recommended ones. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To change the defined security level, perform the following actions:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, set the required security level for the task selected, or click the **Settings** button to modify scan settings manually.

If you modify the settings manually, the name of the security level will change to **Custom**.

To restore the default scan settings:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Default level** button for the task selected.

CREATING THE SCAN STARTUP SCHEDULE

You can create a schedule to automatically start virus scan tasks: specify task run frequency, start time (if necessary), and advanced settings.

If it is not possible to start the task for any reason (for example, the computer was not on at that time), you can configure the skipped task to start automatically as soon as it becomes possible. You can automatically pause the scan when a screensaver is inactive or the computer is unlocked. This functionality postpones the launch until the user has finished working on the computer. The scan will then not take up system resources during the work.

Special Idle Scan mode (see section "Running tasks in background mode" on page 169) allows you to start scan of the system memory, system partition, and startup objects when your computer is idle.

To modify a schedule for scan tasks:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Vulnerability Scan**).
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select **By schedule** and configure the scan run mode.

To enable automatic launch of skipped task:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Vulnerability Scan**).
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select **By schedule** and check the **Run skipped tasks** box.

To launch scans only when the computer is not being used:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Vulnerability Scan**).
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select **By schedule** and check the **Pause scheduled scan when screensaver is inactive and computer is unlocked** box.

CREATING A LIST OF OBJECTS TO SCAN

Each virus scan task has its own default list of objects. These objects may include items in the computer's file system, such as logical drives and **email databases**, or other types of objects such as network drives. You can edit this list.

If the scan scope is empty, or it contains no selected objects, a scan task cannot be started.

To create a list of objects for an object scan task:

1. Open the main application window.
2. In the left part of the window, select the **Scan** section.
3. In the right part of the window click the **select** link to open the list of objects for scanning.
4. In the **Custom Scan** window that opens, click the **Add** button.
5. In the **Select object to scan** window that opens, select the required object and click the **Add** button. Click the **OK** button after you have added all the objects you need. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

   You can also drag files to be scanned directly into a marked area located in the **Scan** section.

To create the list of objects for Full Scan, Critical Areas Scan or Vulnerability Scan tasks:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required scan task (**Full Scan**, **Critical Areas Scan**, or **Vulnerability Scan**).
3. In the right part of the window, click the **Scan scope** button.
4. In the **Scan scope** window that opens, use the **Add**, **Edit**, and **Delete** buttons to create a list. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

   Objects which appear on the list by default cannot be edited or deleted.

SELECTING THE SCAN METHOD

During virus scan, *signature analysis* is always used: Kaspersky Internet Security compares the object found with the database records.

You can use the additional scan methods to increase the scan efficiency: *heuristic analysis* (analysis of the actions an object performs within the system) and *rootkit scan* (tools that can hide malicious programs in your operating system).

To specify which scan method to use:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Additional** tab, in the **Scan methods** section, select the required values for the settings.

SELECTING THE SCAN TECHNOLOGY

In addition to the scan methods you can use special technologies, allowing you to increase the virus scan speed by excluding the files that have not been modified since they were last scanned.

To enable the object scan technologies:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Additional** tab, in the **Scan technologies** section, select the required values.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

If infected or potentially infected objects are detected, the application performs the specified action.

To change the action to be performed on detected objects:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the right part of the window, select the required option in the **Action on threat detection** section.

RUNNING SCAN UNDER A DIFFERENT USER ACCOUNT

By default, the scan tasks are run under your system account. However, you may need to run task under a different user account. You can specify an account to be used by the application when performing a scan task.

To start the scan under a different user's account:

1. Open the application settings window.
2. In the left part of the window, select the required task in the **Scan** (**Full Scan**, **Critical Areas Scan**, **Custom Scan**, or **Vulnerability Scan**) section.
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab, in the **User account** section, check the **Run task as** box. Specify the user name and password.

CHANGING THE TYPE OF OBJECTS TO SCAN

When specifying the type of objects to scan, you establish which file formats and sizes will be scanned for viruses when the selected scan task runs.

When selecting file types please remember the following:

- Probability of malicious code penetrating several file formats (such as .txt) and its further activation is quite low. At the same time, there are formats that contain or may contain an executable code (such as .exe, .dll, .doc). The risk of penetrating and activating malicious code in such files is quite high.

- The intruder can send a virus to your computer in an executable file renamed as txt file. If you have selected the scan of files by extension, such a file is skipped by the scan. If the scan of files by format is selected, then, regardless of the extension, File Anti-Virus will analyze the file header, and reveal that the file is an .exe file. Such a file would be thoroughly scanned for viruses.

To change the type of scanned objects:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Scope** tab, in the **File types** section, select the required option.

SCAN OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, databases, etc. To detect viruses that are hidden in this way a compound file should be unpacked, which can significantly lower the scan speed.

For each type of compound file, you can select to scan either all files or only new ones. To make your selection, click the link next to the name of the object. It changes its value when you left-click on it. If you select the scan new and changed files only scan mode (see page 83), you will not be able to select the links allowing you to scan all or new only files.

You can restrict the maximum size of the compound file being scanned. Compound files larger than the specified value will not be scanned.

When large files are extracted from archives, they will be scanned even if the **Do not unpack large compound files** box is checked.

To modify the list of scanned compound files:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Scope** tab, in the **Scan of compound files** section, select the required types of compound files to be scanned.

In order to set the maximum size of compound files to be scanned:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).

3. In the **Security level** section, click the **Settings** button for the task selected.

4. In the window that opens, on the **Scope** tab, in the **Scan of compound files** section, click the **Additional** button.

5. In the **Compound files** window that opens, check the **Do not unpack large compound files** box and specify the maximum file size.

SCAN OPTIMIZATION

You can shorten the scan time and speed up Kaspersky Internet Security. This can be achieved by scanning only new files and those files that have altered since the last time they were scanned. This mode applies both to simple and compound files.

You can also set a restriction on scan duration for an object. When the specified time interval expires, the object will be excluded from the current scan (except for archives and files comprised of several objects).

To scan only new and changed files:

1. Open the application settings window.

2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).

3. In the **Security level** section, click the **Settings** button for the task selected.

4. In the window that opens, on the **Scope** tab, in the **Scan optimization** section, check the **Scan only new and changed files** box.

To set a restriction on scan duration:

1. Open the application settings window.

2. In the left part of the window, in the **Scan** section, select the required task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).

3. In the **Security level** section, click the **Settings** button for the task selected.

4. In the window that opens, on the **Scope** tab, in the **Scan optimization** section, check the **Skip objects scanned longer than** box and specify the scan duration for a single file.

SCANNING REMOVABLE DRIVES ON CONNECTION

Nowadays, malicious objects using operating systems' vulnerabilities to replicate via networks and removable media have become increasingly widespread. Kaspersky Internet Security allows to scan removable drives when connecting them to the computer.

To configure scanning of removable media at connection:

1. Open the application settings window.

2. In the left part of the window, in the **Scan** section, select **General Settings**.

3. In the **Scan removable drives on connection** section, select the action and define the maximum size of a drive to scan in the field below, if necessary.

CREATING A TASK SHORTCUT

The application provides the option of creating shortcuts for a quick start of full, quick and vulnerability scan tasks. This can start the required scan without opening the main application window or the context menu.

To create a shortcut to start a scan:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select **General Settings**.
3. In the right part of the window, in the **Scan tasks quick run** section, click the **Create shortcut** button next to the name of the required task (**Critical Areas Scan**, **Full Scan**, or **Vulnerability Scan**).
4. Specify the path for saving a shortcut and its name in the window that opens. By default, the shortcut is created with the name of a task in the *My Computer* folder of the current computer user.

VULNERABILITY SCAN

Vulnerabilities of the operating system could be caused by programming or engineering mistakes, unreliable passwords, malicious programs' activity, and so on. When scanning for vulnerabilities, the application analyzes the system, searches for anomalies and damaged settings of the operating system and web browser, looks for vulnerable services and takes other security-related precautions.

The diagnostics may take some time. When it is complete, found problems are analyzed from the perspective of a possible threat to the system.

After the vulnerability scan task start (see page 61), its progress is displayed in the **Vulnerability Scan** window, in the **Finish** field. Vulnerabilities detected when scanning the system and applications, are displayed in the same window, on the **System vulnerabilities** and **Vulnerable applications** tabs.

When searching for threats, information on the results is logged in a Kaspersky Internet Security report.

As with virus scan tasks, you can set a start schedule for a vulnerability scan task, create a list of objects to scan (see page 80), specify an account (see section "Running scan under a different user account" on page 81) and create a shortcut for quick start of a task. By default, the applications already installed on the computer are selected as scan objects.

UPDATE

Updating databases and program modules of Kaspersky Internet Security ensures the up-to-date protection status for your computer. New viruses, Trojans, and other types of malware appear worldwide on a daily basis. Kaspersky Internet Security databases contain information about threats and ways of eliminating them, so regular application update is required for ensuring your computer's security and for timely detection of new threats.

Regular update requires an active license for application usage. Without a license, you will only be able to update the application once.

Application update downloads and installs the following updates on your computer:

- Kaspersky Internet Security databases.

  The protection of information is based on databases which contain signatures of threats and network attacks, and the methods used to fight them. Protection components use these databases to search for and disinfect dangerous objects on your computer. The databases are supplemented every hour with records of new threats. Therefore, you are advised to update them on a regular basis.

In addition to the Kaspersky Internet Security databases, the network drivers that enable the application's components to intercept network traffic are updated.

- Application modules.

  In addition to the databases of Kaspersky Internet Security, you can also update the program modules. The update packages fix Kaspersky Internet Security's vulnerabilities, and supplement or improve the existing functionality.

The main update source of Kaspersky Internet Security are special Kaspersky Lab update servers. While updating Kaspersky Internet Security, you can copy database and program module updates received from Kaspersky Lab servers into a local folder, providing access to other networked computers. This saves Internet traffic.

You can also modify automatic update startup settings.

Your computer should be connected to the Internet for successful downloading of updates from our servers. By default, the Internet connection settings are determined automatically. If you use a proxy server, you may need to adjust the connection settings.

When performing updates (see page 130), the application modules and databases on your computer are compared with the up-to-date version at the update source. If your current databases and modules differ from those in the actual version of the application, the lacking portion of updates will be installed on your computer.

If the databases are outdated, the update package may be large, which may cause additional Internet traffic (up to several dozen MB).

Prior to updating the databases, Kaspersky Internet Security creates backup copies of them if you want to roll back to the previous version of databases.

Information about the current condition of Kaspersky Internet Security databases is displayed in the **Update Center** section of the main application window.

Information on the update results and events, which have occurred during the execution of the update task, is logged in a Kaspersky Internet Security report.

IN THIS SECTION:

Selecting an update source 85

Creating the update startup schedule 87

Rolling back the last update 88

Scanning Quarantine after update 88

Using the proxy server 88

Running updates under a different user account 89

SELECTING AN UPDATE SOURCE

Update source is a resource containing updates for databases and application modules of Kaspersky Internet Security. You can specify HTTP/FTP servers, local and network folders as update sources.

The main update sources are Kaspersky Lab update servers where database updates and application module updates for all Kaspersky Lab products are stored.

If you do not have access to Kaspersky Lab's update servers (for example, the access to the Internet is restricted), you can call the Kaspersky Lab headquarters (http://www.kaspersky.ru/contacts) to request contact information of Kaspersky Lab partners who can provide you with updates on removable media.

When ordering updates on removable media, please specify whether you also require updates for the application modules.

By default, the list of update sources contains only Kaspersky Lab's update servers. If several resources are selected as update sources, Kaspersky Internet Security tries to connect to them one after another, starting from the top of the list, and retrieves the updates from the first available source.

If you select a resource outside the LAN as an update source, you must have an Internet connection to update.

To choose an update source:

1. Open the application settings window.
2. In the left part of the window, in the **Update Center** section, select the **Update Settings** component.
3. Click the **Update source** button in the right part of the window.
4. In the window that opens, on the **Source** tab, open the selection window by clicking the **Add** button.
5. In the **Select update source** window that opens, select the folder that contains the updates, or enter an address in the **Source** field to specify the server from which the updates should be downloaded.

SELECTING THE UPDATE SERVER REGION

If you use Kaspersky Lab servers as the update source, you can select the optimal server location when downloading updates. Kaspersky Lab servers are located in several countries.

Using the closest Kaspersky Lab update server allows you to reduce the time period required for receiving updates and increase the operation performance speed. By default, the application uses information about the current region from the operating system's registry. You can select the region manually.

To select the server region:

1. Open the application settings window.
2. In the left part of the window, in the **Update Center** section, select the **Update Settings** component.
3. Click the **Update source** button in the right part of the window.
4. In the window that opens, on the **Source** tab, in the **Regional settings** section, select the **Select from the list** option, and then select the country nearest to your current location from the dropdown list.

UPDATING THE APPLICATION FROM A SHARED FOLDER

To save Internet traffic, you can configure update of Kaspersky Internet Security from a shared folder when updating the application on networked computers. If done, one of the networked computers receives an update package from Kaspersky Lab servers or from another web resource that contains the required set of updates. The received updates are copied into a shared folder. Other networked computers access this folder to receive updates for Kaspersky Internet Security.

To enable updates distribution mode:

1. Open the application settings window.
2. In the left part of the window, in the **Update Center** section, select the **Update Settings** component.
3. Check the **Copy updates to folder** box in the **Additional** section and specify the path to a public folder where all downloaded updates are copied in the field below. You can also select a folder by clicking the **Browse** button.

To enable updating the application on a specified computer from the shared folder you have selected:

1. Open the application settings window.
2. In the left part of the window, in the **Update Center** section, select the **Update Settings** component.
3. Click the **Update source** button in the right part of the window.
4. In the window that opens, on the **Source** tab, open the selection window by clicking the **Add** button.
5. In the **Select update source** window that opens, select a folder or enter the full path to it in the **Source** field.
6. Uncheck the **Kaspersky Lab update servers** box on the **Source** tab.

CREATING THE UPDATE STARTUP SCHEDULE

You can create a schedule to automatically start an update task: specify task run frequency, start time (if necessary), and advanced settings.

If it is not possible to start the task for any reason (for example, the computer was not on at that time), you can configure the skipped task to start automatically as soon as it becomes possible.

You can also postpone automatic startup of the task after the application is started. Note that all scheduled tasks will be run only after the specified time interval elapses since the startup of Kaspersky Internet Security.

Special Idle Scan mode (see section "Running tasks in background mode" on page 169) allows you to start automatic update keeping your computer idle.

To configure the update task startup schedule:

1. Open the application settings window.
2. In the left part of the window, in the **Update Center** section, select the **Update Settings** component.
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select the **By schedule** option and configure the update run mode.

To enable automatic launch of skipped task:

1. Open the application settings window.
2. In the left part of the window, in the **Update Center** section, select the **Update Settings** component.
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select **By schedule** and check the **Run skipped tasks** box.

To postpone task run after the application startup:

1. Open the application settings window.
2. In the left part of the window, in the **Update Center** section, select the **Update Settings** component.
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select the **By schedule** option and fill in the **Postpone running after application startup for** field to specify the time to which the task run should be postponed.

ROLLING BACK THE LAST UPDATE

After first update of Kaspersky Internet Security databases and program modules, the option of rolling back to the previous databases becomes available.

At the start of the update process, Kaspersky Internet Security creates a backup copy of the current databases and application modules. If necessary, you can restore the previous databases. Update roll back feature is useful in case the new databases version contains an invalid signature that makes Kaspersky Internet Security block a safe application.

In the event of Kaspersky Internet Security database damage it is recommended to launch update to download a valid set of databases for up-to-date protection.

To roll back to the previous database version:

1. Open the main application window.
2. Select the **Update Center** section in the left part of the window.
3. Click the **Roll back to the previous databases** button in the right part of the window.

SCANNING QUARANTINE AFTER UPDATE

If the application has scanned an object and has not found out what malicious programs have infected it, the object is quarantined. After the next database update, the product may be able to recognize the threat unambiguously and neutralize it. You can enable the auto scan for quarantined objects after each update.

For this reason, the application scans quarantined objects after each update. Scanning may change their status. Some objects can then be restored to the previous locations, and you will be able to continue working with them.

To enable scanning quarantined files after update:

1. Open the application settings window.
2. In the left part of the window, in the **Update Center** section, select the **Update Settings** component.
3. Check the **Rescan Quarantine after update** box in the **Additional** section.

USING THE PROXY SERVER

If you use a proxy server for Internet connection, you should reconfigure it to allow proper update of Kaspersky Internet Security.

To configure the proxy server:

1. Open the application settings window.

2. In the left part of the window, in the **Update Center** section, select the **Update Settings** component.
3. Click the **Update source** button in the right part of the window.
4. In the window that opens, on the **Source** tab, click the **Proxy server** button.
5. Configure the proxy server settings in the **Proxy server settings** window that opens.

RUNNING UPDATES UNDER A DIFFERENT USER ACCOUNT

By default, the update procedure is run under your system account. However, Kaspersky Internet Security can update from a source for which you have no access rights (for example, from a network folder containing updates) or authorized proxy user credentials. You can run Kaspersky Internet Security updates on behalf of the user account that has such rights.

To start the update under a different user's account:

1. Open the application settings window.
2. In the left part of the window, in the **Update Center** section, select the **Update Settings** component.
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab, in the **User account** section, check the **Run task as** box. Specify the user name and password.

FILE ANTI-VIRUS

File Anti-Virus prevents infection of the computer's file system. The component starts upon startup of the operating system, continuously remains in the computer's RAM, and scans all files being opened, saved, or launched on your computer and all connected drives.

You can create the protection scope and set the security level (collection of settings that determine the scan's thoroughness).

When the user or a program attempts to access a protected file, File Anti-Virus checks if the iChecker and iSwift databases contain information about this file, and makes a decision on whether the file should be scanned or not.

By default, the mode of using records from application databases to search for threats is always enabled. Additionally, you can apply heuristic analysis (see page 92) and various scan technologies (see page 93).

If a threat is detected, Kaspersky Internet Security assigns one of the following statuses to the found object:

- malicious program (such as a *virus* or *Trojan*);
- *potentially infected* (suspicious) status if the scan cannot determine whether the object is infected or not. The file may contain a sequence of code appropriate for viruses, or modified code from a known virus.

The application displays a notification about detected threat and performs the assigned action. You can change actions to be performed on detected threat.

If you work in automatic mode (see section "Selecting protection mode" on page 76), Kaspersky Internet Security will automatically apply the action recommended by Kaspersky Lab specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Move to Quarantine**.

Before attempting to disinfect or delete an infected object, Kaspersky Internet Security creates a backup copy for subsequent restoration or disinfection. Suspicious (potentially infected) objects are quarantined. You can enable the automatic scan of quarantined objects after each update.

IN THIS SECTION:

Enabling and disabling File Anti-Virus 90

Automatically pausing File Anti-Virus 90

Creating a protection scope 91

Changing and restoring security level 92

Selecting scan mode 92

Using heuristic analysis 92

Selecting the scan technology 93

Changing actions to be performed on detected objects 93

Scan of compound files 93

Scan optimization 94

ENABLING AND DISABLING FILE ANTI-VIRUS

By default, File Anti-Virus is enabled, functioning in normal mode. You can disable File Anti-Virus, if necessary.

To disable File Anti-Virus:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the right part of the window, uncheck the **Enable File Anti-Virus** box.

AUTOMATICALLY PAUSING FILE ANTI-VIRUS

When carrying out resource-intensive works, you can pause File Anti-Virus. To reduce workload and ensure quick access to objects, you can configure automatic pausing of the component at a specified time or when handling specified programs.

Pausing File Anti-Virus when it conflicts with some programs is an emergency operation! If any conflicts arise when working with the component, please contact Kaspersky Lab Technical Support Service (http://support.kaspersky.com). The support specialists will help you resolve the simultaneous operation of Kaspersky Internet Security with other applications on your computer.

To pause the component at a specified time:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. Click the **Settings** button in the **Security level** section in the right part of the window.
4. In the window that opens, on the **Additional** tab, in the **Pause task** section, check the **By schedule** box and click the **Schedule** button.

5. In the **Pause task** window, specify the time (in 24-hour hh:mm format) for which protection will be paused (**Pause task at** and **Resume task at** fields).

To pause the component when running specified applications:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. Click the **Settings** button in the **Security level** section in the right part of the window.
4. In the window that opens, on the **Additional** tab, in the **Pause task** section, check the **At application startup** box and click the **Select** button.
5. In the **Applications** window create a list of applications which pause the component when running.

CREATING A PROTECTION SCOPE

Protection scope is the location of objects being scanned and the types of files to be scanned. By default, Kaspersky Internet Security scans only potentially infectable files stored on any hard drive, network drive or removable media.

You can expand or restrict the protection scope by adding / removing objects to be scanned or changing the type of files to be scanned. For example, you can only select EXE files run from network drives to be scanned.

When selecting file types please remember the following:

- Probability of malicious code penetrating several file formats (such as .txt) and its further activation is quite low. At the same time, there are formats that contain or may contain an executable code (such as .exe, .dll, .doc). The risk of penetrating and activating malicious code in such files is quite high.
- The intruder can send a virus to your computer in an executable file renamed as txt file. If you have selected the scan of files by extension, such a file is skipped by the scan. If the scan of files by format is selected, then, regardless of the extension, File Anti-Virus will analyze the file header, and reveal that the file is an .exe file. Such a file would be thoroughly scanned for viruses.

To edit the object scan list:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **General** tab, in the **Protection scope** section, open the object selection window by clicking the **Add** link.
5. In the **Select object to scan** window, select an object and click the **Add** button.
6. After you have added all required objects, click the **OK** button in the **Select object to scan** window.
7. To remove an object from the scan list, uncheck the box next to it.

To change the type of scanned objects:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **General** tab, in the **File types** section, select the required settings.

CHANGING AND RESTORING SECURITY LEVEL

Depending on your actual needs, you can select one of the preset file/memory security levels or configure File Anti-Virus on your own.

When configuring File Anti-Virus, you can always roll back to the recommended settings. These settings are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To change the current file and memory security level:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the right part of the window, in the **Security level** section, set the required security level, or click the **Settings** button to modify the settings manually.

If you modify the settings manually, the name of the security level will change to **Custom**.

To restore the default protection settings:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. Click the **Default level** button in the **Security level** section in the right part of the window.

SELECTING SCAN MODE

The scan mode is the condition which triggers File Anti-Virus into activity. The default setting for Kaspersky Internet Security is smart mode, which determines if the object is subject to scanning on the basis of the actions performed in respect of it. For example, when working with a Microsoft Office document, Kaspersky Internet Security scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned.

You can change the object scan mode. The scan mode should be selected depending on the files you work with most of the time.

To change the object scan mode:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. Click the **Settings** button in the **Security level** section in the right part of the window.
4. In the window that opens on the **Additional** tab, in the **Scan mode** section, select the required mode.

USING HEURISTIC ANALYSIS

During File Anti-Virus operation, *signature analysis* is always used: Kaspersky Internet Security compares the object found with the database records.

To improve protection efficiency, you can use the *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis allows detecting new malicious objects which are not yet described in the databases.

To enable the heuristic analysis:

1. Open the application settings window.

2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.

3. Click the **Settings** button in the **Security level** section in the right part of the window.

4. In the window that opens, on the **Performance** tab, in the **Scan methods** section, check the **Heuristic analysis** box and specify the detail level for the scan.

SELECTING THE SCAN TECHNOLOGY

In addition to the heuristic analysis you can use special technologies, allowing an increase in the objects scan speed by excluding the files that have not been modified since they were last scanned.

To enable the object scan technologies:

1. Open the application settings window.

2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.

3. Click the **Settings** button in the **Security level** section in the right part of the window.

4. In the window that opens, on the **Additional** tab, in the **Scan technologies** section, select the required values.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

If infected or potentially infected objects are detected, the application performs the specified action.

To change the specified action to be performed on detected objects:

1. Open the application settings window.

2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.

3. In the right part of the window, select the required option in the **Action on threat detection** section.

SCAN OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, databases, etc. To detect viruses that are hidden in this way a compound file should be unpacked, which can significantly lower the scan speed.

For each type of compound file, you can select to scan either all files or only new ones. To make your selection, click the link next to the name of the object. It changes its value when you left-click on it. If you select the scan new and changed files only scan mode (see page 94), you will not be able to select the links allowing you to scan all or new only files.

By default, Kaspersky Internet Security scans only embedded OLE objects.

When large compound files are scanned, their preliminary unpacking may take a long period of time. This period can be reduced by enabling unpacking of compound files in background mode if they exceed the specified file size. If a malicious object is detected while working with such a file, the application will notify you about it.

You can restrict the maximum size of the compound file being scanned. Compound files larger than the specified value will not be scanned.

When large files are extracted from archives, they will be scanned even if the **Do not unpack large compound files** box is checked.

- *To modify the list of scanned compound files:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
  3. Click the **Settings** button in the **Security level** section in the right part of the window.
  4. In the window that opens, on the **Performance** tab, in the **Scan of compound files** section, select the required type of compound files to be scanned.

- *In order to set the maximum size of compound files to be scanned:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
  3. Click the **Settings** button in the **Security level** section in the right part of the window.
  4. In the window that opens, on the **Performance** tab, in the **Scan of compound files** section, click the **Additional** button.
  5. In the **Compound files** window, check the **Do not unpack large compound files** box and specify the maximum file size.

- *To unpack large-sized compound files in background mode:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
  3. Click the **Settings** button in the **Security level** section in the right part of the window.
  4. In the window that opens, on the **Performance** tab, in the **Scan of compound files** section, click the **Additional** button.
  5. In the **Compound files** window, check the **Extract compound files in the background** box and specify the minimum file size.

SCAN OPTIMIZATION

You can shorten the scan time and speed up Kaspersky Internet Security. This can be achieved by scanning only new files and those files that have altered since the last time they were scanned. This mode applies both to simple and compound files.

- *To scan only new and changed files:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
  3. Click the **Settings** button in the right part of the window.
  4. In the window that opens, on the **Performance** tab, in the **Scan optimization** section, check the **Scan only new and changed files** box.

MAIL ANTI-VIRUS

Mail Anti-Virus scans incoming and outgoing messages for malicious objects. It starts when the operating system boots and runs continually, scanning all email messages sent or received via the POP3, SMTP, IMAP, MAPI, and NNTP protocols, as well as over encrypted connections (SSL) via POP3 and IMAP (see section "Scanning encrypted connections" on page 128).

The indicator of the component's operation is the application icon in the taskbar notification area, which looks like whenever an email message is being scanned.

You can specify the types of messages which should be scanned and select the security level (see page 97) (configuration settings affecting the scan intensity).

The application intercepts each message that the user sends or receives and parses it into basic components: message header, body, attachments. Message body and attachments (including attached OLE objects) are scanned for the presence of threats.

By default, the mode of using records from application databases to search for threats is always enabled. In addition, you can enable heuristic analysis. Furthermore, you can enable filtering of attachments (see page 98), which allows automatic renaming or deletion of specified file types.

If a threat is detected, Kaspersky Internet Security assigns one of the following statuses to the found object:

- malicious program (such as a *virus* or *Trojan*);
- *potentially infected* (suspicious) status if the scan cannot determine whether the object is infected or not. The file may contain a sequence of code appropriate for viruses, or modified code from a known virus.

The application blocks a message, displays a notification about detected threat and performs the assigned action. You can change actions to be performed on detected threat (see section "Changing actions to be performed on detected objects" on page 98).

If you work in automatic mode (see section "Selecting protection mode" on page 76), Kaspersky Internet Security will automatically apply the action recommended by Kaspersky Lab specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Move to Quarantine**.

Before attempting to disinfect or delete an infected object, Kaspersky Internet Security creates a backup copy for subsequent restoration or disinfection. Suspicious (potentially infected) objects are quarantined. You can enable the automatic scan for quarantined objects after each update.

After the email message is successfully disinfected, it returns to the user. If the disinfection fails, the infected object is deleted from the message. After the virus scan, a special text is inserted in the subject line of the email, stating that the email was processed by Kaspersky Internet Security.

An integrated plug-in is provided for Microsoft Office Outlook (see section "Email scanning in Microsoft Office Outlook" on page 99) that allows you to fine-tune the email client.

If you use The Bat!, Kaspersky Internet Security can be used in conjunction with other anti-virus applications. At that, the email traffic processing rules (see section "Email scanning in The Bat!" on page 99) are configured directly in The Bat! and override the application's email protection settings.

When working with other mail programs, including Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora, and Incredimail, the Mail Anti-Virus component scans email on SMTP, POP3, IMAP, and NNTP protocols.

Note that when working with the Thunderbird mail client, email messages transferred via IMAP will not be scanned for viruses if any filters moving messages from the **Inbox** folder are used.

IN THIS SECTION:

Enabling and disabling Mail Anti-Virus 96

Creating a protection scope 96

Changing and restoring security level 97

Using heuristic analysis 97

Changing actions to be performed on detected objects 98

Attachment filtering 98

Scan of compound files 98

Email scanning in Microsoft Office Outlook 99

Email scanning in The Bat! 99

ENABLING AND DISABLING MAIL ANTI-VIRUS

By default, Mail Anti-Virus is enabled, functioning in normal mode. You can disable Mail Anti-Virus, if necessary.

- *To disable Mail Anti-Virus:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
  3. In the right part of the window, uncheck the **Enable Mail Anti-Virus** box.

CREATING A PROTECTION SCOPE

Protection scope is understood as the type of messages to be scanned. By default, Kaspersky Internet Security scans both incoming and outgoing emails.

If you have selected scan only incoming messages, you are advised to scan outgoing email when you first begin using Kaspersky Internet Security since it is likely that there are worms on your computer which will distribute themselves via email. This will avoid unpleasant situations caused by unmonitored mass emailing of infected emails from your computer.

The protection scope also includes the settings used to integrate the Mail Anti-Virus component into the system, and the protocols to be scanned. By default, the Mail Anti-Virus component is integrated into the Microsoft Office Outlook and The Bat! email client applications.

- *To disable scans of outgoing emails:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
  3. Click the **Settings** button in the right part of the window.
  4. Use the **General** tab of the displayed window to select in the **Protection scope** section the option **Incoming messages only**.

To select the protocols to scan and the settings to integrate Mail Anti-Virus into the system:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Additional** tab, in the **Connectivity** section select the required settings.

CHANGING AND RESTORING SECURITY LEVEL

Depending on your actual needs, you can select one of the preset email security levels or configure Mail Anti-Virus on your own.

Kaspersky Lab advises you not to configure Mail Anti-Virus settings on your own. In most cases, it is enough to select a different security level.

When configuring Mail Anti-Virus, you can always roll back to the recommended values. These settings are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To change the preset email security level:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. In the right part of the window, in the **Security level** section, set the required security level, or click the **Settings** button to modify the settings manually.

If you modify the settings manually, the name of the security level will change to **Custom**.

To restore default mail protection settings:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. Click the **Default level** button in the **Security level** section in the right part of the window.

USING HEURISTIC ANALYSIS

During Mail Anti-Virus operation, *signature analysis* is always used: Kaspersky Internet Security compares the object found with the database records.

To improve protection efficiency, you can use the *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis allows detecting new malicious objects which are not yet described in the databases.

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **General** tab, in the **Scan methods** section, check the **Heuristic analysis** box and specify the detail level for the scan.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

If infected or potentially infected objects are detected, the application performs the specified action.

To change the specified action to be performed on detected objects:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. In the right part of the window, select the required option in the **Action on threat detection** section.

ATTACHMENT FILTERING

Malware is most often distributed in mail as objects attached to messages. To protect your computer, for example, from automatic launch of attached files, you can enable filtering of attachments, which can automatically rename or delete files of specified types.

To enable filtering of attachments:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. Use the **Attachment filter** tab of the displayed window to select the filtering mode for attachments. When you select either of the last two modes, the list of file types (extensions) will become enabled; there you can select the required types or add a mask to select a new type.

   To add a new type mask to the list, click the **Add** link to open the **Input file name mask** window and enter the necessary information.

SCAN OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, databases, etc. To detect viruses that are hidden in this way a compound file should be unpacked, which can significantly lower the scan speed.

You can enable or disable the scan of attached archives and limit the maximum size of archives to be scanned.

If your computer is not protected by any local network software (you access the Internet directly without a proxy server or a firewall), it is not recommended to disable the scanning of attached archives.

To configure the settings for the scan of compound files:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. Use the **General** tab in the displayed window to define necessary settings.

EMAIL SCANNING IN MICROSOFT OFFICE OUTLOOK

If you are using Microsoft Office Outlook as your mail client, you may modify additional settings for scanning your mail for viruses.

When installing Kaspersky Internet Security, a special plug-in is installed in Microsoft Office Outlook. It allows you to configure Mail Anti-Virus settings quickly, and determine when email messages are scanned for dangerous objects.

The plug-in comes in the form of **Email protection** tab located in the **Tools** → **Options** menu.

To define the proper time for mail scanning, perform the following steps:

1. Open the main Microsoft Outlook application window.
2. Select **Tools** → **Options** from the application menu.
3. Use the **Email protection** tab to select necessary settings.

EMAIL SCANNING IN THE BAT!

Actions in respect of infected email objects in The Bat! are defined using the application's own tools.

Mail Anti-Virus settings determining if incoming and outgoing messages should be scanned, which actions should be performed in respect of dangerous objects in email, and which exclusions should apply, are ignored. The only thing that The Bat! takes into account is the scanning of attached archives.

The email protection settings extend to all the anti-virus components installed on the computer that support working with the Bat!.

Note that incoming email messages are first scanned by Mail Anti-Virus and only after that – by the plug-in of The Bat!. If a malicious object is detected, Kaspersky Internet Security immediately notifies you of this event. If you select the **Disinfect** (**Delete**) action in the notification window of Mail Anti-Virus, actions aimed at eliminating the threat are performed by Mail Anti-Virus. If you select the **Ignore** option in the notification window, the object will be disinfected by the plug-in of The Bat!. When sending email messages, they are first scanned by the plug-in and then - by Mail Anti-Virus.

You have to define the following criteria:

- which mail stream (incoming, outgoing) should be scanned;
- when the mail objects should be scanned (when opening a message, before saving to disk);
- what actions are performed by the mail client if dangerous objects are detected in email messages. For example, you could select:
  - **Attempt to disinfect infected parts** – if this option is selected, the attempt is made to disinfect the infected object; if it cannot be disinfected, the object remains in the message.
  - **Delete infected parts** – if this option is selected, the dangerous object in the message is deleted regardless of whether it is infected or suspected to be infected.

By default, The Bat! places all infected email objects in Quarantine without attempting to disinfect them.

The Bat! does not give special headers to emails containing dangerous objects.

To set up email protection rules in The Bat!:

1. Open the main The Bat! window.

2. Select the **Settings** item from the **Properties** menu of the mail client.

3. Select the **Virus protection** object from the settings tree.

WEB ANTI-VIRUS

Whenever you use the Internet, the information stored on your computer becomes subject to the risk of infection from dangerous programs. These can infiltrate your computer while you are downloading free software, or browsing known safe websites, which have been subject to hacker attacks before you have gone on them. Moreover, network worms can penetrate your computer before you open a webpage or download a file just because your computer is connected to the Internet.

The *Web Anti-Virus* component is designed to ensure security while using the Internet. It protects your computer against data coming in via the HTTP, HTTPS and FTP protocols, and also prevents dangerous scripts from being executed on the computer.

Web protection monitors the data stream that passes only through the ports included in the monitored port list. A list of ports that are most commonly used for data transfer is included in the Kaspersky Internet Security installation package. If you use any ports that are not included in this list, add them into the list of monitored ports (see section "Creating a list of monitored ports" on page 131) to ensure protection of data streams being directed via them.

A collection of settings called the security level defines how the data stream will be scanned (see section "Selecting the Web Anti-Virus security level" on page 102). If Web Anti-Virus detects a threat, it will perform the assigned action.

Kaspersky Lab advises you not to configure Web Anti-Virus settings on your own. In most cases, it is enough to select an appropriate security level.

Component operation algorithm

Web Anti-Virus protects the data reaching your computer and transferred from it over HTTP, HTTPS and FTP, and prevents hazardous scripts from running on the computer. By default, scan of secure connections (via HTTPS) is disabled, you can enable and configure it (see section "Scanning encrypted connections" on page 128).

Data is protected using the following algorithm:

1. Each web page or file that is accessed by the user or an application via the HTTP, HTTPS or FTP protocols, is intercepted and analyzed for malicious code by Web Anti-Virus. Malicious objects are detected using both Kaspersky Internet Security databases and the heuristic algorithm. The database contains descriptions of all the malicious programs known to date and methods for neutralizing them. The heuristic algorithm can detect new viruses that have not yet been entered in the database.

2. After the analysis, you have the following courses of action available:

   - If a web page or an object accessed by the user contains malicious code, access to them is blocked. A notification is displayed that the object or page being requested is infected.

   - If the file or web page does not contain malicious code, the program immediately grants the user access to it.

Scripts are scanned according to the following algorithm:

1. Each script run is intercepted by Web Anti-Virus and is analyzed for malicious code.

2. If the script contains malicious code, Web Anti-Virus blocks this script and informs the user of it with a special pop-up message.

3. If no malicious code is discovered in the script, it is run.

Web Anti-Virus intercepts only scripts using the Microsoft Windows Script Host functionality.

IN THIS SECTION:

Enabling and disabling Web Anti-Virus 101

Selecting the Web Anti-Virus security level 102

Changing actions to be performed on dangerous objects 102

Checking URLs using the databases of suspicious and phishing addresses 102

Using heuristic analysis 103

Blocking dangerous scripts 104

Scan optimization 104

Kaspersky URL Advisor 104

Blocking access to dangerous websites 105

Control requests to regional domains 106

Controlling access to online banking services 106

Creating a list of trusted addresses 107

Restoring Web Anti-Virus default settings 107

ENABLING AND DISABLING WEB ANTI-VIRUS

There are two ways to enable or disable the component:

- from the main application window (see section "Kaspersky Internet Security main window" on page 44);
- from the settings window (see section "Application settings window" on page 48).

To enable or disable Web Anti-Virus in the main window, perform the following steps:

1. Open the main application window and select the **Protection Center** section in the left part of the window.
2. In the right part of the window, left-click to open the **Online Security** or the **System and Applications Protection** section.
3. Open the menu for selecting an action to take on the component by clicking the **Web Anti-Virus** button and select **Enable Web Anti-Virus** (if the component should be enabled) or **Disable Web Anti-Virus** (if it should be disabled).

   When enabling a component, the icon on its left turns green and when disabling it, the icon turns grey.

To enable or disable Web Anti-Virus in the settings window:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Check the **Enable Web Anti-Virus** box in the right part of the window, if the component should be enabled. Uncheck the box if the component should be disabled.

SELECTING THE WEB ANTI-VIRUS SECURITY LEVEL

The security level is defined as a preset configuration of the Web Anti-Virus settings providing for a certain level of protection for the data received and transmitted over HTTP, HTTPS and FTP. Kaspersky Lab specialists distinguish three security levels:

- High level provides maximum protection necessary while working in dangerous environment.
- Recommended level provides optimal protection recommended in most cases.
- Low level allows maximum performance.

The user should decide which level to select according to the working conditions and the current situation.

To select one of the preset security levels, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Use the slider in the right part of the window to choose the required security level.

If none of the preset levels satisfies your requirements, you can configure the Web Anti-Virus, for example, modify the level of scanning intensity during heuristic analysis. Such configuration will change the security level name to **Custom**.

If you need to revert again to a preset security level, simply restore the default settings of the component (see section "Restoring Web Anti-Virus default settings" on page 107).

CHANGING ACTIONS TO BE PERFORMED ON DANGEROUS OBJECTS

Once analysis of a web traffic object shows that it contains malicious code, the response by the Web Anti-Virus component depends on the action you have selected.

Web Anti-Virus always blocks actions by dangerous scripts and issues messages that inform the user of the action taken. The action on a dangerous script cannot be changed – the only available modification is disabling scan of scripts (see section "Blocking dangerous scripts" on page 104).

If you are working in automatic mode, then Kaspersky Internet Security automatically applies the action recommended by Kaspersky Lab's specialists when dangerous objects are detected.

To select the action to be performed on detected objects:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. In the **Action on threat detection** section in the right part of the window, choose the action, which the application should perform with the discovered dangerous object.

CHECKING URLS USING THE DATABASES OF SUSPICIOUS AND PHISHING ADDRESSES

Web Anti-Virus can scan web traffic for viruses and also check URLs to make sure they are not present in the lists of suspicious or phishing web addresses.

Checking the links if they are included in the list of phishing addresses allows avoiding phishing attacks, which look like email messages from would-be financial institutions and contain links to the websites of these organizations. The message text convinces the reader to click the link and enter confidential information in the window that follows, for

example, a credit card number or a login and password for an Internet banking site where financial operations may be carried out. A phishing attack can be disguised, for example, as a letter from your bank with a link to its official website. By clicking the link, you go to an exact copy of the bank's website and can even see the real address in the browser, even though you are actually on a counterfeit site. From this point forward, all your actions on the site are tracked and can be used to steal your money.

The lists of phishing URLs are included with the Kaspersky Internet Security delivery set. Since links to phishing web sites may be received not only in email, but also from other sources, such as ICQ messages, Web Anti-Virus monitors attempts to access a phishing web site on the level of web traffic and blocks access to such locations.

To configure Web Anti-Virus to check URLs against the databases of suspicious and phishing web addresses, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

   The **Web Anti-Virus** window opens.
4. In the **Scan methods** section of the **General** tab, make sure that the boxes **Check if URLs are listed in the database of suspicious URLs** and **Check if URLs are listed in the database of phishing URLs** are selected.

USING HEURISTIC ANALYSIS

Heuristic analysis is a special inspection method. It is used to analyze the activity of an object within the host system. If that activity is typical of harmful objects, then such object will be recognized as malicious or suspicious with sufficient probability even if the dangerous code in it is yet unknown to the anti-virus analysts.

You can select the level of heuristic analysis intensity:

- light scan – a quick check;
- deep scan – a thorough check taking more time;
- medium scan – an optimal combination of scanning speed and depth suitable in most cases.

If heuristic analysis reveals a malicious object, Kaspersky Internet Security will notify you about that and suggest appropriate handling for the detected object.

Heuristic analysis is enabled by default, the intensity level is set to **medium scan**.

To enable heuristic analysis and define its intensity level or disable it, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

   The **Web Anti-Virus** window opens.
4. To enable heuristic analysis, go to the **General** tab and check in the **Scan methods** section the **Heuristic analysis** box. Use the slider below to define the necessary scanning intensity level. Uncheck the **Heuristic Analysis** box if that scanning method should not be used.

BLOCKING DANGEROUS SCRIPTS

Web Anti-Virus can scan all scripts processed in Microsoft Internet Explorer, as well as any other WSH scripts (JavaScript, Visual Basic Script, etc.) launched when the user works on the computer. If a script presents a threat to your computer, it will be blocked.

In order for Web Anti-Virus to scan and block scripts:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

   The **Web Anti-Virus** window opens.
4. Make sure that the **Block dangerous scripts in Microsoft Internet Explorer** box is checked on the **General** tab in the **Additional** section.

SCAN OPTIMIZATION

To detect malicious code more efficiently, Web Anti-Virus caches fragments of objects downloaded from the Internet. When using this method, Web Anti-Virus only scans an object after it has been completely downloaded. The object is then scanned for viruses and returned to the user for work or blocked, depending on the scan results.

Caching objects increases object processing time, and hence the time before the application returns objects to the user. Caching can cause problems when downloading or processing large objects, as the connection with the HTTP client may time out.

To solve this problem, we suggest limiting the caching time for the object fragments downloaded from the Internet. When a specified period of time expires, the user will receive the downloaded part of the object without scanning, and once the object is fully copied, it will be scanned in full. This allows reducing the time needed to transfer the object to the user and eliminating the disconnection problem. The Internet security level will not be reduced in that case.

Removing the limit of caching time results in improved efficiency of anti-virus scan though causing a slight slowdown of access to the object.

To set a time limit for fragment buffering or remove it:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

   The **Web Anti-Virus** window opens.
4. To restrict the traffic scanning duration, on the **General** tab check in the **Additional** section the **Limit traffic caching time to optimize scan** box. Uncheck the box, if you need to cancel the restriction.

KASPERSKY URL ADVISOR

Kaspersky Internet Security includes the URL scanning module managed by Web Anti-Virus. This module is built into Microsoft Internet Explorer and Mozilla Firefox browsers as a plug-in.

This module checks if links located on the webpage belong to the list of suspicious and phishing web addresses. You can create a list of web addresses whose content will not be checked for the presence of suspicious or phishing URLs, or a list of web sites whose content must be scanned. You can also completely exclude scan of URLs.

The below-listed options of Kaspersky URL Advisor configuration can be selected not only in the application settings window but also in the advisor module settings window that you open from your web browser.

- *To create a list of websites whose content will not be scanned for the presence of suspicious or phishing URLs:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
  3. Click the **Settings** button in the right part of the window.

     The **Web Anti-Virus** window opens.
  4. On the **Safe Surf** tab in the **Kaspersky URL Advisor** section, select the **On all web pages except the exclusions** option and click the **Exclusions** button.
  5. Use the displayed **Exclusions** window to create the list of web sites whose content will not be scanned for the presence of suspicious or phishing URLs.

- *To create a list of websites whose content should be scanned for suspicious or phishing URLs:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
  3. Click the **Settings** button in the right part of the window.

     The **Web Anti-Virus** window opens.
  4. On the **Safe Surf** tab in the **Kaspersky URL advisor** section, select the **On the selected web pages** option and click the **Select** button.
  5. Use the displayed **Checked URLs** window to create the list of web addresses whose content must be checked for the presence of suspicious or phishing URLs.

- *If you want no URLs to be checked by the advisor:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
  3. Click the **Settings** button in the right part of the window.

     The **Web Anti-Virus** window opens.
  4. On the **Safe Surf** tab, in the **Kaspersky URL Advisor** section, check the **Scan URLs** box.

- *To open the Kaspersky URL Advisor settings window from your web browser,*

  click the button with the Kaspersky Internet Security icon in the browser toolbar.

BLOCKING ACCESS TO DANGEROUS WEBSITES

You can block access to websites which have been considered as suspicious or phishing by Kaspersky URL advisor (see section "Kaspersky URL advisor" on page 104).

If the application cannot make a clear decision on security of a website to which the URL redirects, you are offered to load this website in Safe Run for Websites mode (see page 155) (only for Microsoft Internet Explorer, Mozilla Firefox browsers). When running in Safe Run mode, malicious objects do not pose any threat to your computer.

To block access to dangerous websites:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

   The **Web Anti-Virus** window opens.
4. On the **Safe Surf** tab, in the **Block dangerous websites** section, check the **Block dangerous websites** box.

CONTROL REQUESTS TO REGIONAL DOMAINS

Depending on the user's choice, Web Anti-Virus in Geo Filter mode can block or allow access to websites on the grounds of their belonging to regional web domains. This allows you, for example, to block access to websites which belong to regional domains with a high risk of infection.

To allow or block access to websites which belong to specified domains:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

   The **Web Anti-Virus** window opens.
4. On the **Geo Filter** tab, check the **Enable filtering by regional domains** box and specify in the list of controlled domains below which domains should be allowed or blocked, and for which ones the application should request access permission using a notification (see section "Requesting for permission of accessing a website from a regional domain" on page 201).

   By default, access is allowed for regional domains that match your location. Access permission request is set for other domains by default.

CONTROLLING ACCESS TO ONLINE BANKING SERVICES

When working with online banking, the user needs special protection, since leakages of confidential information may lead to financial losses. Web Anti-Virus can control access to online banking services, thus ensuring safe interaction with them (see section "Safe Run for Websites" on page 155). Web Anti-Virus automatically defines which web resources are online banking services. For guaranteed identification of a web resource as online banking service, you can specify its URL in the corresponding list.

To enable control of access to online banking services:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

   The **Web Anti-Virus** window opens.
4. On the **Online Banking** tab, check the **Enable control** box. You are offered to start the Certificate Installation Wizard that you can use to install the Kaspersky Lab certificate for scanning encrypted connections.
5. If required, create a list of resources that should be necessarily identified as online banking services by the application.

CREATING A LIST OF TRUSTED ADDRESSES

You can create a list of web addresses whose content you unconditionally trust. Web Anti-Virus will not analyze data from those addresses for dangerous objects. This option may be useful, for instance, when Web Anti-Virus interferes with downloading a particular file from a known website.

To create the list of trusted web addresses:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

   The **Web Anti-Virus** window opens.
4. On the **Trusted URLs** tab, check the **Do not scan web traffic from trusted URLs** box and create a list of URLs providing trusted content.

If you need to exclude an address from the trusted list temporarily, you do not have to delete it – unchecking its box to the left will produce the necessary effect.

RESTORING WEB ANTI-VIRUS DEFAULT SETTINGS

If you are not satisfied with the reconfigured behavior of Web Anti-Virus, you can restore the component configuration advised by Kaspersky Lab. These settings are combined in the **Recommended** security level.

To restore default Web Anti-Virus settings:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Default level** button in the **Security level** section in the right part of the window.

   Security level will be set to **Recommended**.

IM ANTI-VIRUS

IM Anti-Virus scans the traffic of instant messaging clients (the so-called *Internet pagers*).

IM messages may contain links to suspicious web sites and to the web sites deliberately used by hackers to organize phishing attacks. Malicious programs use IM clients to send spam messages and links to the programs (or the programs themselves), which steal users' ID numbers and passwords.

Kaspersky Internet Security ensures safe operation of various instant messaging applications, including ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent and IRC.

Some IM clients, such as Yahoo! Messenger and Google Talk use a secure connection. To scan the traffic generated by those programs, you have to enable scanning for secure connections (see page 128).

IM Anti-Virus intercepts the messages checking them for the presence of dangerous objects or URLs. You can select the types of messages (see page 108) to scan and various scanning methods.

If threats are detected in a message, IM Anti-Virus substitutes this message with a warning message for the user.

Files transferred via IM clients are scanned by the File Anti-Virus component when attempts are made to save them.

IN THIS SECTION:

Enabling and disabling IM Anti-Virus 108

Creating a protection scope 108

Selecting the scan method 108

ENABLING AND DISABLING IM ANTI-VIRUS

By default, IM Anti-Virus is enabled, functioning in normal mode. You can disable IM Anti-Virus, if necessary.

To disable IM Anti-Virus:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
3. In the right part of the window, uncheck the **Enable IM Anti-Virus** box.

CREATING A PROTECTION SCOPE

Protection scope is understood as the type of messages to be scanned. By default, Kaspersky Internet Security scans both incoming and outgoing emails. If you are sure that messages sent by you cannot contain any dangerous objects, you may disable the scan of outgoing traffic.

To disable the scan of outgoing messages:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
3. In the right part of the window, in the **Protection scope** section, select the **Incoming messages only** option.

SELECTING THE SCAN METHOD

Scan methods consist of scanning the URLs in IM clients' messages to know if they are included in the list of suspicious web addresses and / or in the list of phishing web addresses.

To improve protection efficiency, you can use the *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis allows detecting new malicious objects which are not yet described in the databases. When using heuristic analysis, any script included in an IM client's message is executed in a protected environment. If this script's activity is typical of malicious objects, the object is likely to be classed as malicious or suspicious. By default, heuristic analysis is enabled.

To scan links in the messages using the database of suspicious web addresses:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
3. In the right part of the window, in the **Scan methods** section, check the **Check if URLs are listed in the database of suspicious URLs** box.

To scan links in the messages using the database of phishing web addresses:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
3. In the right part of the window, in the **Scan methods** section, check the **Check if URLs are listed in the database of phishing URLs** box.

To enable the heuristic analysis:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
3. In the right part of the window, in the **Scan methods** section, check the **Heuristic analysis** box and define the necessary scanning intensity level.

PROACTIVE DEFENSE

Proactive Defense ensures protection against new threats which are not yet included in Kaspersky Internet Security databases.

The preventative technologies provided by Proactive Defense neutralize new threats before they harm your computer. In contrast with responsive technologies, which analyze code based on records in Kaspersky Internet Security databases, preventative technologies recognize a new threat on your computer by the sequence of actions executed by a program. If, as a result of activity analysis, the sequence of an application's actions arouses suspicion, Kaspersky Internet Security blocks the activity of this application.

For example, when actions such as a program copying itself to network resources, the startup folder and the system registry are detected, it is highly likely that this program is a worm. Hazardous sequences of actions also include attempts to modify the HOSTS file, hidden installation of drivers, etc. You can turn off monitoring (see page 110) for any hazardous activity or edit the rules of monitoring (see page 110) for it.

As opposed to the Application Control, Proactive Defense responds immediately to a defined sequence of an application's actions. Activity analysis is performed for all applications, including those grouped as **Trusted** by the Application Control component.

You can create a group of trusted applications (see page 110) for Proactive Defense. If done, you will not be notified of activities of these applications.

If your computer runs under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7, or Microsoft Windows 7 x64, control will not apply to each event. This is due to specific features of these operating systems. For example, control will not apply in full volume to the sending data through trusted applications, and suspicious system activities.

IN THIS SECTION:

Enabling and disabling Proactive Defense 110

Creating a group of trusted applications 110

Using the dangerous activity list 110

Changing the dangerous activity monitoring rule 110

ENABLING AND DISABLING PROACTIVE DEFENSE

By default, Proactive Defense is enabled, functioning in optimum mode. You can disable Proactive Defense, if required.

To disable Proactive Defense:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.
3. In the right part of the window, uncheck the **Enable Proactive Defense** box.

CREATING A GROUP OF TRUSTED APPLICATIONS

Programs recognized by the Application Control component as **Trusted** pose no threat for the system. However, their activities will also be monitored by Proactive Defense. You can create a group of trusted applications; Proactive Defense will not monitor their activity. By default, the list of trusted applications includes applications with verified digital signature and applications from Kaspersky Security Network database.

To change the settings of the trusted applications group, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.
3. In the right part of the window, in the **Trusted applications** section, check the boxes next to the required settings.

USING THE DANGEROUS ACTIVITY LIST

The list of actions typical of dangerous activity cannot be edited. You can turn off monitoring for one dangerous activity or another.

To turn off monitoring for one dangerous activity or another:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.
3. Click the **Settings** button in the right part of the window.
4. In the **Proactive Defense** window that opens, uncheck the box next to the type of activity which you do not want to be monitored.

CHANGING THE DANGEROUS ACTIVITY MONITORING RULE

Applications' actions classified as dangerous activity cannot be edited. You can perform the following actions:

- turn off monitoring for any activity (see page 110);
- create an exclusion list (see page 167), by listing applications the activities of which you do not consider dangerous;
- edit the rule that Proactive Defense uses when it detects dangerous activity;

To edit Proactive Defense rule:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.
3. Click the **Settings** button in the right part of the window.
4. In the **Proactive Defense** window that opens, in the **Event** column, select the required event for which you want to edit the rule.
5. Configure the settings for the selected event using the links in the **Rule description** section. For example:
   a. click the link with the preset action and, in the **Select action** window that opens, select the required action;
   b. click the **On / Off** link to indicate that a report on task execution should be created.

SYSTEM WATCHER

System Watcher collects data about applications actions on your computer and provides information to other components for improved protection.

If saving applications' activity logs is enabled, System Watcher allows you to roll back actions performed by malicious programs (see page 112). Rolling back actions after malicious activity is detected in the system can be initiated either by the System Watcher component based on patterns of dangerous activity (see section "Using patterns of dangerous activity (BSS)" on page 112), or by Proactive Defense, and during virus scan task run or File Anti-Virus operation (see page 89).

The component's response to matching between applications' actions and patterns of dangerous activity and rollback of malicious programs' actions depend on Kaspersky Internet Security's mode of operation.

If suspicious actions are detected in the system, Kaspersky Internet Security protection components can request Activity monitor for additional information. When Kaspersky Internet Security runs in interactive mode, you can view the event data collected by the System Watcher component in a dangerous activity report, which helps you make a decision when selecting actions in the notification window. When the component detects a malicious program, the link to the System Watcher's report is displayed in the top part of the notification window (see page 201), prompting you for action.

IN THIS SECTION:

Enabling and disabling System Watcher 111

Using patterns of dangerous activity (BSS) 112

Rolling back a malicious program's actions 112

ENABLING AND DISABLING SYSTEM WATCHER

By default, System Watcher is enabled, running in a mode that depends on the current mode of Kaspersky Internet Security – automatic or interactive.

You are advised to avoid disabling the component, except for emergency cases, since this inevitably impacts efficiency of Proactive Defense and other protection components operation that may request the data collected by Activity monitor in order to identify the potential threat detected.

To disable System Watcher:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **System Watcher** component.
3. In the right part of the window, uncheck the **Enable System Watcher** box.

USING PATTERNS OF DANGEROUS ACTIVITY (BSS)

Patterns of dangerous activity (BSS – Behavior Stream Signatures) contain sequences of actions typical of applications classified as dangerous. If an application's activity matches a pattern of dangerous activity, Kaspersky Internet Security performs the specified action.

When Kaspersky Internet Security is updated, patterns of activity used by Activity monitor are supplied with new ones on-the-fly for up-to-date and reliable protection.

By default, when Kaspersky Internet Security runs in automatic mode, if an application's activity matches a pattern of dangerous activity, System Watcher moves this application to Quarantine. When running in interactive mode (see page 76), System Watcher prompts the user for action. You can specify the action that the component should perform when an application's activity matches a pattern of dangerous activity.

In addition to exact matching between applications' activities and patterns of dangerous activity, System Watcher also detects actions that partly match patterns of dangerous activity, being considered suspicious based on the heuristic analysis. If suspicious activity is detected, System Watcher prompts the user for action regardless of the operation mode.

To select the action that the component should perform if an application's activity matches a pattern of dangerous activity:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **System Watcher** component.
3. In the right part of the window, in the **Heuristic analysis** section, check the **Use updatable patterns of dangerous activity (BSS)** box.
4. Click **Select action** and then specify the required action on the dropdown list.

ROLLING BACK A MALICIOUS PROGRAM'S ACTIONS

You can use the product feature for rolling back the actions performed by malware in the system. To enable a roll-back, System Watcher should log the history of program activity.

By default, Kaspersky Internet Security rolls back relevant operations automatically when the protection components detect malicious activity. When running in interactive mode (see page 76), System Watcher prompts the user for action. You can specify the operation which should be performed whenever malicious activity is detected.

The procedure of rolling back malware operations affects a strictly defined set of data. It causes no negative consequences for the operating system or data integrity on your computer.

To configure rollback of malware operations, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **System Watcher** component.
3. In the right part of the window, in the **Applications activity log** section check the **Save activity log** box.
4. Click **Select action** and then specify the required action on the dropdown list.

APPLICATION CONTROL

Application Control prevents applications from performing actions that may be dangerous for the system, and ensures control of access to operating system resources and your identity data.

The component tracks actions in the system performed by applications installed on the computer, and regulates them based on the rules of Application Control. These rules regulate potentially dangerous activity, including applications' access to protected resources, such as files and folders, registry keys, and network addresses.

Applications' network activity is controlled by the Firewall component (see page 121).

At the first startup of an application on the computer, the Application Control component verifies its safety and includes it into one of the trust groups. The trust group defines the rules that Kaspersky Internet Security should apply to control the activity of this application. Rules of Application Control is a set of rights of access to the computer resources and restrictions posed on various actions being performed by applications on the computer.

You can configure the conditions for distribution of applications by groups (see page 114), move an application to another group (see page 115), or edit the rules of Kaspersky Internet Security (see page 116).

We recommend that you participate in Kaspersky Security Network in order to improve performance of Application Control. Data obtained using Kaspersky Security Network allow you to distribute applications by groups with more accuracy and apply optimum rules of Application Control.

When the application is restarted, Application Control checks its integrity. If the application has not been changed, the component applies the current rule to it. If the application has been modified, Application Control re-scans it as at the first startup.

To control applications' access to various resources of your computer, you can use the preset list of protected resources or add user resources to the list (see page 119).

IN THIS SECTION:

Enabling and disabling Application Control 113

Placing applications into groups 114

Viewing activity of applications 115

Modifying a trust group and restoring default group 115

Working with rules of Application Control 116

Protecting operating system resources and identity data 119

Interpreting the data of application usage by the participants of Kaspersky Security Network 120

ENABLING AND DISABLING APPLICATION CONTROL

By default, Application Control is enabled, functioning in the mode developed by Kaspersky Lab specialists. However, you can disable it, if required.

To disable Application Control:

1. Open the main application window and select the **Protection Center** section in the left part of the window.

2. In the right part of the window, left-click to open the **System and Applications Protection** list of components.

3. Select the **Application Control** component.

4. In the menu that opens, select **Disable Application Control**.

PLACING APPLICATIONS INTO GROUPS

At the first startup of an application on the computer, the Application Control component verifies its safety and includes it into one of the trust groups.

At the first stage of the application scan, Kaspersky Internet Security searches the internal database of known applications for a matching entry, and then sends a request to the Kaspersky Security Network database (see section "Participating in the Kaspersky Security Network" on page 185) (if an Internet connection is available). If an entry of that application is found in the database, the application is included into a group registered in the database.

Applications that do not pose any threat to the system are included into the **Trusted** group. By default, this group includes applications with a digital signature and applications whose parent objects have one. You can disable the automatic inclusion of applications with a digital signature into the **Trusted** group.

Behavior of applications included into the **Trusted** group will however be controlled by the Proactive Defense component (on page 109).

By default, Kaspersky Internet Security uses the heuristic analysis to distribute unknown applications (not included into the Kaspersky Security Network database and functioning without a digital signature) by groups. The analysis helps defining the threat rating of the application based on which it is included into a group. Instead of using the heuristic analysis, you can specify a group into which Kaspersky Internet Security should automatically include all unknown applications.

By default, Application Control analyzes an application for 30 seconds. If this time interval turns out to be insufficient for defining the threat rating, the application is included into the **Low restricted** group, while defining the threat rating continues in background mode. After that, the application is finally included into another group. You can change the time allocated for application analysis. If you are sure that all applications started on your computer do not pose any threat to its security, you can decrease the time spent on analysis. If, on the contrary, you are installing the software and are not sure that this is safe, you are advised to increase the time for analysis.

If the application threat rating is high, Kaspersky Internet Security notifies you about it and offers you to select a group where to place the application. Notification (see page 199) contains statistics of the application use by Kaspersky Security Network participants. Based on the statistics and with regard for the history of emergence of this application on your computer, you can make a weighted decision on the group into which the application should be included (see section "Interpreting the data of application usage by the participants of Kaspersky Security Network" on page 120).

- *To disable the automatic inclusion of applications with a digital signature into the **Trusted** group:*

  1. Open the application settings window.

  2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.

  3. In the right part of the window, in the **Applications restriction** section, uncheck the **Trust applications with digital signature** box.

- *To use the heuristic analysis for distributing unknown applications by groups:*

  1. Open the application settings window.

  2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.

  3. In the right part of the window, in the **Applications restriction** section, select **Use the heuristic analysis to define group**.

To change the time allowed for calculation of the group:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
3. In the right part of the window, in the **Applications restriction** section, edit the value of the **Maximum time to define the application group** setting.

To include all unknown applications into the specified group:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
3. In the right part of the window, in the **Applications restriction** section, select **Move to the following group automatically** and specify the required group from the dropdown list.

VIEWING ACTIVITY OF APPLICATIONS

You can view information about all applications being used on your computer and all processes being currently run.

To view applications' activity:

1. Open the main application window and select the **Protection Center** section.
2. In the right part of the window, left-click to open the **System and Applications Protection** list of components.
3. Click the **Applications Activity** link.
4. In the **Applications Activity** window that opens, in the top left corner, select the required category of applications from the dropdown list.

MODIFYING A TRUST GROUP AND RESTORING DEFAULT GROUP

At the first startup of an application, Kaspersky Internet Security automatically includes it into a group (see section "Placing applications into groups" on page 114). If necessary, you can move the application to another group manually. At any moment, you can move the application back to the default group.

Kaspersky Lab specialists recommend that you avoid moving applications from default groups. Instead, if required, edit the rules for an individual application (see section "Editing application rules" on page 117).

To move an application to another group:

1. Open the main application window and select the **Protection Center** section.
2. In the right part of the window, left-click to open the **System and Applications Protection** list of components.
3. Click the **Applications Activity** link.
4. In the **Applications Activity** window that opens, in the top left corner, select the required category of applications from the dropdown list.
5. Right-click to open the context menu for the required application and select **Move to group** → **<group name>**.

To roll back to the status assigned to the application automatically:

1. Open the main application window and select the **Protection Center** section.

2. In the right part of the window, left-click to open the **System and Applications Protection** list of components.

3. Click the **Applications Activity** link.

4. In the **Applications Activity** window that opens, in the top left corner, select the required category of applications from the dropdown list.

5. Right-click to open the context menu for the required application and select **Move to group** → **Restore default group**.

WORKING WITH RULES OF APPLICATION CONTROL

Rules of Application Control is a set of rights of access to the computer resources and restrictions posed on various actions being performed by applications on the computer.

By default, an application is controlled according to the rules of the trust group into which Kaspersky Internet Security included the application when it was run for the first time. Group rules have been developed by Kaspersky Lab specialists for an optimum control of applications' activity. If necessary, you can edit these rules or adjust them for an individual application. Rules of an application have a higher priority than rules of a group.

IN THIS SECTION:

Editing group rules 116

Editing application rules 117

Loading rules from Kaspersky Security Network 118

Inheritance of restrictions of the parent process 118

Deleting rules for unused applications 119

EDITING GROUP RULES

By default, different trust groups have different optimum sets of rights of access to the computer resources. You can edit the preset group rules.

To change the group rule:

1. Open the application settings window.

2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.

3. In the right part of the window, in the **Configure application rules and protected resources** section, click the **Applications** button.

4. In the **Applications** window that opens, select the required group from the list and click the **Edit** button.

5. In the **Group rules** window that opens, select the tab that match the required resource category (**Files and system registry**, **Rights**).

6. Right-click the column with the respective action on the required resource to open the context menu and select the required value (**Allow**, **Block**, or **Prompt for action**).

EDITING APPLICATION RULES

You can modify restrictions at the level of an individual application or exclude some actions from the rules for an application. Kaspersky Internet Security will not control actions that have been added to exclusions from the rules for an application.

All exclusions created in the rules for applications are available in the application settings window (see section "Application settings window" on page 48) in the **Threats and Exclusions** section.

You can also disable the applying of group rules to the control of access to the selected categories of protected resources. The access to these resources is managed by the application rules.

To change an application rule:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
3. In the right part of the window, in the **Configure application rules and protected resources** section, click the **Applications** button.
4. In the **Applications** window that opens, select the required application from the list and click the **Edit** button.
5. In the **Application rules** window that opens, select the tab that match the required resource category (**Files and system registry**, **Rights**).
6. Right-click the column with the respective action on the required resource to open the context menu and select the required value (**Allow**, **Block**, or **Prompt for action**).

To disable the inheritance of group rules for access to resources:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
3. In the right part of the window, in the **Configure application rules and protected resources** section, click the **Applications** button.
4. In the **Applications** window that opens, select the required application from the list.
5. Click the **Edit** button.
6. In the **Application rules** window that opens, select the tab that match the required resource category (**Files and system registry**, **Rights**).
7. For the necessary resource, right-click the corresponding action column to open the context menu and select in it the **Inherit** item with the box checked.

To add an exclusion to the application rules:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
3. In the right part of the window, in the **Configure application rules and protected resources** section, click the **Applications** button.
4. In the **Applications** window that opens, select the required application from the list and click the **Edit** button.
5. In the **Application rules** window that opens, select the **Exclusions** tab.
6. Check the boxes for the actions that should not be controlled.

LOADING RULES FROM KASPERSKY SECURITY NETWORK

By default, applications found in the Kaspersky Security Network database are processed according to the rules loaded from this database.

If an application had not been found in the Kaspersky Security Network database at the first run but information about it was added later, Kaspersky Internet Security will automatically update the rules for the control of this application by default.

You can disable the loading of rules from Kaspersky Security Network and / or the automatic update of the rules for previously unknown applications.

- *To disable the downloads of rules from Kaspersky Security Network:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
  3. In the left part of the window, in the **Applications restriction** section, uncheck the **Load rules for applications from Kaspersky Security Network (KSN)** box.

- *Do disable the updates of Kaspersky Security Network rules for previously unknown applications:*

  1. Open the application settings window.
  2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
  3. In the right part of the window, in the **Applications restriction** section, uncheck the **Update rules for previously unknown applications from KSN** box.

INHERITANCE OF RESTRICTIONS OF THE PARENT PROCESS

Application startup may be initiated either by the user or by another application running. If the startup is initiated by another application, it creates a startup procedure including parent and child applications.

When an application attempts to obtain access to a protected resource, Application Control analyzes the rights of all parent processes of this application, and compares them to the rights required to access this resource. The minimum priority rule is then observed: when comparing the access rights of the application to those of the parent process, the access rights with a minimum priority will be applied to the application's activity.

Access right priority:

1. Allow. Access right data has the highest priority.
2. Prompt for action.
3. Block. Access right data has the lowest priority.

This mechanism prevents a non-trusted application or an application with restricted rights from using a trusted application to perform actions requiring certain privileges.

If an application's activity is blocked because a parent process has insufficient rights, you can edit these rules (see section "Editing application rules" on page 117) or disable inheritance of restrictions from the parent process.

You should modify the rights of a parent process only if you are absolutely certain that the process' activities do not threaten the security of the system.

To disable inheritance of restrictions from the parent process, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
3. In the right part of the window, in the **Configure application rules and protected resources** section, click the **Applications** button.
4. In the **Applications** window that opens, select the required application from the list.
5. Click the **Edit** button.
6. In the **Application rules** window that opens, select the **Exclusions** tab.
7. Check the **Do not inherit restrictions of the parent process (application)** box.

DELETING RULES FOR UNUSED APPLICATIONS

By default, the rules for applications which have not been started for the 60 days are deleted automatically. You can modify the storage time for rules for unused applications, or disable rules' automatic removal.

To set the storage time for application rules:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
3. In the right part of the window, check the **Delete rules for applications remaining inactive for more than** box in the **Additional** section and specify the necessary number of days.

To disable the automatic removal of the rules for unused applications:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
3. In the right part of the window, in the **Additional** section, uncheck the **Delete rules for applications remaining inactive for more than** box.

PROTECTING OPERATING SYSTEM RESOURCES AND IDENTITY DATA

Application Control manages the applications' rights to take actions on various resource categories of the operating system and identity data.

Kaspersky Lab specialists have distinguished the preset categories of protected resources. You cannot edit this list. However, you can expand this list by adding user categories and / or individual resources, or stop controlling the selected resources.

In addition, you can add specified resources to exclusions. Access to those resources will not be controlled.

To add identity data to be protected:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.
3. Click the **Resources** button in the right part of the window.

4. In the window that opens, on the **Identity data** tab, select the required category of identity data from the dropdown list and open the window for adding resources by clicking the **Add** button.

5. In the **User resource** window that opens, specify the required settings based on the resource being added.

After you add a resource, you can edit or remove it using the respective buttons in the top part of the tab. To disable the control of a resource or category, uncheck the box next to it.

To create the category of identity data items to be protected:

1. Open the application settings window.

2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.

3. Click the **Resources** button in the right part of the window.

4. In the window that opens, on the **Identity data** tab, open the window for adding resource categories by clicking the **Add category** button.

5. In the **Identity data category** window that opens, enter a name for the new resource category.

To add operating system settings and resources to be protected:

1. Open the application settings window.

2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.

3. Click the **Resources** button in the right part of the window.

4. In the window that opens, on the **Operating system** tab, select the required category of operating system objects from the **Category** dropdown list.

5. Click the **Add** button and select the required type of resource from the menu that opens.

6. In the **User resource** window that opens, specify the required settings based on the resource being added.

After you add a resource, you can edit or remove it using the respective buttons in the top part of the tab. To disable the control of a resource or category, uncheck the box next to it.

To add a resource to the exclusion list:

1. Open the application settings window.

2. In the left part of the window, in the **Protection Center** section, select the **Application Control** component.

3. Click the **Resources** button in the right part of the window.

4. In the window that opens, on the **Exclusions** tab, click the **Add** button and select the required resource type from the menu that opens.

5. In the **User resource** window that opens, specify the required settings based on the resource being added.

INTERPRETING THE DATA OF APPLICATION USAGE BY THE PARTICIPANTS OF KASPERSKY SECURITY NETWORK

Information about the application usage by the participants of Kaspersky Security Network (see page 185) will allow you to make a weighted decision on which status should be assigned to an application running on your computer. To assess maliciousness or safety of an application with a great precision based on KSN data, you should be aware of the events that have led to the emergence of this application on your computer.

Kaspersky Lab specialists distinguish the following sources of new applications:

- the user downloads a setup file from the Internet and then opens it;
- a setup file is automatically downloaded and opened when the user clicks a link on a web page;
- the user opens a setup file stored on a CD / DVD or copied to the hard disk from it;
- the user opens a setup file stored on a USB drive or copied to the hard disk from it;
- the user opens a setup file received in a message via email, IM client, or social network.

Statistics of application usage by the participants of Kaspersky Security Network includes frequency and remoteness of usage of an application. Below are the main options of application usage:

- **very rarely** (less than 100 participants of KSN use this application) and **recently** (the file has appeared a few days ago);
- **rarely** (less than 1,000 participants of KSN) and relatively **long ago** (a few months ago), most users restrict the activity of this application;
- **frequently** (more than 100,000 participants of KSN) and **long ago** (more than six months ago), most users trust this application;
- **frequently** (more than 100,000 participants of KSN) and **recently** (a few weeks ago), most users trust or restrict this application;
- **very frequently** (more than 100,000 participants of KSN) and **recently**, most users trust this application.

NETWORK PROTECTION

Various protection components, tools, and settings of Kaspersky Internet Security together ensure security and control of your network activities.

The sections below contain detailed information about the principles of operation and configuration of Firewall, Network Attack Blocker, Network Monitor, scan of secure connections, proxy server settings, and monitoring of network ports.

IN THIS SECTION:

Firewall 121

Network Attack Blocker 126

Encrypted connections scan 128

Network Monitor 130

Configuring the proxy server 130

Creating a list of monitored ports 131

FIREWALL

The Firewall ensures security for your work in local networks and on the Internet.

The component filters the entire network activity according to the network rules of Application Control. Network rule is an action that Firewall performs when it detects a connection attempt with a specified status. Status is assigned to each network connection; it is defined by specified settings: data transfer direction and protocol, addresses and ports to which the connection is established.

The Firewall analyzes the settings of the networks to which you connect your computer. If the application runs in interactive mode, Firewall, when first connected, requests you for the status of the connected network (see page 200). If interactive mode is off, the Firewall defines the status based on the network type, ranges of addresses and other specifications. You can change the status (see page 122) of a network connection manually.

IN THIS SECTION:

Enabling and disabling Firewall 122

Changing the network status 122

Working with Firewall rules 122

Configuring notifications of changes in the network 125

Advanced Firewall settings 125

ENABLING AND DISABLING FIREWALL

By default, the Firewall is enabled, functioning in normal mode. You can disable the Firewall if needed.

To disable the Firewall:

1. Open the main application window and select the Firewall section in the left part of the window.
2. In the right part of the window, left-click to open the **System and Applications Protection** list of components.
3. Select the **Firewall** component.
4. In the menu that opens, select **Disable Firewall**.

CHANGING THE NETWORK STATUS

The network connection status affects the set of rules used to filter network activity for that connection. You can change the network status, if necessary.

To change the network connection status:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Networks** tab, select an active network connection and click the **Edit** button to open the network settings window.
5. In the window that opens, select the required status from the drop-down list on the **Properties** tab.

WORKING WITH FIREWALL RULES

The Firewall operates on the basis of two types of rules:

- *Packet rules.* They are used for posing restrictions on packets regardless of the application. Typically, such rules restrict incoming network activity on specified TCP and UDP ports and filter ICMP messages.

- *Application rules*. They are used to set limits on network activity of a specified application. Such rules allow fine-tuning the activity filtering, for example, when a certain type of network connections is banned for some applications but is allowed for others.

Packet rules have higher priority than application rules. If both packet rules and rules for applications are applied to the same type of network activity, this network activity is processed using the packet rules. Besides, you can set a priority for each rule (see page 124).

CREATING A PACKET RULE

Packet rules consist of a set of conditions and operations over packets performed when these conditions are met.

When creating packet rules, remember that they have priority over the rules for applications.

To create a packet rule:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Packet rules** tab, open the network rule creation window by clicking the **Add** button.
5. In the **Network rule** window that opens, specify the required settings and click the **OK** button.
6. Assign a priority to the new rule by moving it up or down the list clicking the **Move up** and **Move down** buttons.

   Once you have created the rule, you can modify its settings or delete it using buttons in the top part of the tab. To disable the rule, uncheck the box next to the rule's name.

EDITING GROUP RULES

Similarly to the Application Control component (on page 113), Firewall's default feature is to filter network activity of an application using the rules of the group in which this application has been included.

Network rules of a trust group define which rights of access to various networks can be granted to the applications that have been included in this group. You can add new network rules for a group or edit the preset ones.

To add a network rule for a group:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Application rules** tab, select the required group from the list and click the **Edit** button.
5. In the **Group rules** window that opens, select the **Network rules** tab and click the **Add** button.
6. In the **Network rule** window that opens, specify the required settings and click the **OK** button.
7. Assign a priority to the new rule by moving it up or down the list clicking the **Move up** and **Move down** buttons.

   Once you have created the rule, you can modify its settings or delete it using the buttons in the top part of the tab. To disable the rule, uncheck the box next to the rule's name.

To change a network rule for a group:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Application rules** tab, select the required group from the list and click the **Edit** button.
5. In the **Group rules** window that opens, select the **Network rules** tab.
6. Right-click the **Permission** column to open the context menu for the required rule and select a value: **Allow**, **Block**, or **Prompt for action**.

EDITING APPLICATION RULES

You can create network rules for individual applications. Network rules of an application have a higher priority than network rules of a group.

If necessary, you can create network rules for applications using the Application Control component.

To create a network application rule:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Application rules** tab, select an application and click the **Edit** button to open the rules configuration window.
5. In the window that opens, on the **Network rules** tab, open the window for creating a network rule for the application by clicking the **Add** button.
6. In the **Network rule** window that opens, specify the required settings and click the **OK** button.
7. Assign a priority to the new rule by moving it up or down the list clicking the **Move up** and **Move down** buttons.

   Once you have created the rule, you can modify its settings or delete it using buttons in the top part of the tab. To disable the rule, uncheck the box next to the rule's name.

CHANGING THE RULE PRIORITY

The priority of a rule is defined by its position in the list. The first rule on the list has the highest priority.

Each packet rule created manually is added to the end of the list of packet rules.

Rules for applications are grouped by application name, and the rule priority applies to an individual group only. Rules for applications created manually have higher priority than inherited group rules.

To change the packet rule priority:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button in the right part of the window.

4. In the window that opens, on the **Packet rules** tab, select a rule and move it to the required position on the list by clicking the **Move up** or **Move down** buttons.

To change the application rules priority:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Application rules** tab, select an application and open the rules configuration window by clicking the **Edit** button.
5. In the window that opens, on the **Network rules** tab, select a rule and move it to the required position on the list by clicking the **Move up** or **Move down** buttons.

CONFIGURING NOTIFICATIONS OF CHANGES IN THE NETWORK

Network connection settings can be changed during operation. You can receive notifications of modifications in the settings.

To enable notification about changes to network connection settings:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Networks** tab, select an active network connection and open the network settings window by clicking the **Edit** button.
5. In the window that opens, check the boxes for those events about which you wish to receive notifications on the **Additional** tab.

ADVANCED FIREWALL SETTINGS

You can specify the advanced settings for the Firewall, such as permission of FTP's active mode, connection blockage if no prompt for action is available (application interface is not loaded), and functioning until the system shutdown.

By default, all the settings are enabled.

To modify advanced settings of the Firewall:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Firewall** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Packet rules** tab, open the advanced settings window by clicking the **Additional** button.
5. In the **Additional** window that opens, check / uncheck the boxes next to the required settings.

NETWORK ATTACK BLOCKER

Network Attack Blocker scans inbound traffic for activity typical of network attacks. Once an attempt to attack your computer is detected, Kaspersky Internet Security blocks any network activity of the computer making an attack towards your computer.

By default, the blocking persists for one hour. You can edit the blockage settings (see page 127). A warning will appear on the screen stating that an attempted network attack has taken place, with specific information about the computer which attacked you. Descriptions of currently known network attacks (see section "Types of detected network attacks" on page 126) and methods to fight them, are provided in Kaspersky Internet Security databases. The list of attacks which the Network Attack Blocker can detect is updated when the application's databases are updated (see section "Update" on page 84).

IN THIS SECTION:

Types of detected network attacks 126

Enabling and disabling Network Attack Blocker 127

Editing the blockage settings 127

TYPES OF DETECTED NETWORK ATTACKS

Nowadays, a great number of network attacks exist. These attacks exploit vulnerabilities of the operating system and other software, system-type or otherwise, installed on your computer.

To ensure the security of your computer, you must know what kinds of network attacks you might encounter. Known network attacks can be divided into three major groups:

- *Port scan* – this threat type is not an attack itself but it usually precedes one, since it is one of the common ways of obtaining information about a remote computer. The UDP/TCP ports used by the network tools on the computer targeted by an intruder are scanned to find out their status (closed or open).

  Port scans can tell a hacker what types of attacks work on that system, and what types do not. In addition, the information obtained by the scan (a model of the system) helps the malefactor to know what operating system the remote computer uses. This, in turn, further restricts the number of potential attacks, and, correspondingly, the time spent perpetrating them. It also aids a hacker in attempting to use vulnerabilities characteristic of the operating system.

- *DoS attacks*, or Denial of Service attacks are attacks which cause an unstable performance of a system or its crash. Attacks of this type may affect the operability of information resources under attack (for example, blocking Internet access).

  There are two basic types of DoS attacks:

  - sending the target computer specially created packets that the computer does not expect, which cause the system either to restart or to stop;

  - sending the target computer many packets within a timeframe that the computer cannot process, which causes system resources to be exhausted.

  The most flagrant examples for this group of attacks are the following types:

  - The *Ping of death* attack consists of sending an ICMP packet with a size greater than the maximum of 64 KB. This attack can crash some operating systems.

  - *Land attack* consists of sending a request to an open port on the target computer to establish a connection with itself. This attack sends the computer into a cycle, which intensifies the load on the processor and can lead to the crashing of some operating systems.

- The *ICMP Flood* attack consists of sending a large quantity of ICMP packets to your computer. The computer attempts to reply to each inbound packet, which slows the processor to a crawl.

- The *SYN Flood* attack consists of sending a large quantity of queries to a remote computer to establish a fake connection. The system reserves certain resources for each of those connections, which completely drains your system resources, and the computer stops reacting to other connection attempts.

- *Intrusion attacks*, which aim to take over your computer. This is the most dangerous type of attack, because if it is successful, the hacker takes total control of your system.

  Hackers use this attack to obtain confidential information from a remote computer (for example, credit card numbers, passwords), or to penetrate the system to use its computing resources for malicious purposes later (e.g., to use the invaded system in a zombie network, or as a platform for new attacks).

  This group is the largest in number of attacks included. They may be divided into three groups depending on the operating system installed on the user's computer: Microsoft Windows attacks, Unix attacks, and the common group for network services available in both operating systems.

  The following types of attacks are the most common among those using the network resources of operating systems:

  - *Buffer overflow attacks*. Buffer overflow may be caused by lack (or insufficiency) of control when working with data arrays. This is one of the oldest vulnerability types and the easiest for hackers to exploit.

  - *Format string attacks*. Format string errors arise from insufficient control of input values for I/O functions, such as *printf()*, *fprintf()*, *scanf()*, and others, from the standard C library. If an application has this vulnerability, the hacker is able to send queries created with a special technique and can take total control of the system.

    Intrusion Detection System automatically analyzes and prevents attempts to exploit these vulnerabilities in the most common network services (FTP, POP3, IMAP) if they are running on the user's computer.

  - *Attacks aimed at computers with Microsoft Windows* are based on the use of vulnerabilities of the software installed on a computer (such as Microsoft SQL Server, Microsoft Internet Explorer, Messenger, and system components available via the network – DCom, SMB, Wins, LSASS, IIS5).

  In addition, the use of various malicious scripts, including scripts processed by Microsoft Internet Explorer and Helkern-type worms, can be classified as isolated incidents of intrusion attacks. The essence of this attack type consists of sending a special type of UDP packets to a remote computer that can execute malicious code.

ENABLING AND DISABLING NETWORK ATTACK BLOCKER

By default, Network Attack Blocker is enabled, functioning in optimum mode. You can disable Network Attack Blocker, if necessary.

To disable Network Attack Blocker:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Network Attack Blocker** component.
3. In the right part of the window, uncheck the **Enable Network Attack Blocker** box.

EDITING THE BLOCKAGE SETTINGS

By default, Network Attack Blocker blocks the activity of a computer making an attack for one hour. You can cancel blockage of the selected computer or change the time of blockage.

To modify the time for which the computer making an attack will be blocked:

1. Open the application settings window.

2. In the left part of the window, in the **Protection Center** section, select the **Network Attack Blocker** component.

3. In the right part of the window, check the **Add the attacking computer to the list of blocked computers for** box and specify the time of blockage.

To unblock the computer making an attack:

1. Open the main application window and select the **Protection Center** section.

2. In the right part of the window, left-click to open the **Online Security** list of components.

3. Click the **Network Monitor** link.

4. In the **Network Monitor** window that opens, on the **Blocked computers** tab, select the blocked computer and click the **Unblock** button.

EENCRYPTED CONNECTIONS SCAN

Connecting using the SSL/TLS protocols protects data exchange channel on the Internet. The SSL/TLS protocols allows identifying the parties exchanging data using electronic certificates, encoding the data being transferred, and ensuring their integrity during the transfer.

These features of the protocol are used by hackers to spread malicious programs, since most antivirus applications do not scan SSL/TLS traffic.

Kaspersky Internet Security scans encrypted connections using a Kaspersky Lab's certificate.

If an invalid certificate is detected when connecting to the server (for example, if the certificate is replaced by an intruder), a notification will pop up containing a suggestion to either accept or reject the certificate.

If you are sure that connection with a website is always secure, in spite of an invalid certificate, you can add the website into the list of trusted URLs (see section "Creating a list of trusted addresses" on page 107). Kaspersky Internet Security will no longer scan the encrypted connection with this website.

You can use the Certificate Installation Wizard to install a certificate to scan encrypted connections in semi-interactive mode in Microsoft Internet Explorer, Mozilla Firefox (if it is not launched) and Google Chrome, as well as to get instructions on installing Kaspersky Lab's certificate for Opera.

To enable encrypted connections scan and install the Kaspersky Lab certificate:

1. Open the application settings window.

2. In the left part of the window, in the **Advanced Settings** section, select the **Network** component.

3. In the window that opens check the **Scan encrypted connections** box. When you first enable this setting, the Certificate Installation Wizard starts automatically.

4. If the wizard does not start, click the **Install certificate** button. This will start a wizard with instructions to follow for a successful installation of the Kaspersky Lab certificate.

IN THIS SECTION:

Scanning encrypted connections in Mozilla Firefox..... 129

Scanning encrypted connections in Opera..... 129

SCANNING ENCRYPTED CONNECTIONS IN MOZILLA FIREFOX

Mozilla Firefox browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Firefox, you should install the Kaspersky Lab's certificate manually.

You can use the Certificate Installation Wizard, if the browser is not launched.

- *To install the Kaspersky Lab's certificate manually:*

  1. In the browser menu, select the **Tools** → **Settings** item.
  2. In the window that opens, select the **Additional** section.
  3. In the **Certificates** section, select the **Security** tab and click the **View Certificates** button.
  4. In the window that opens, select the **Authorities** tab and click the **Restore** button.
  5. In the window that opens, select the Kaspersky Lab certificate file. The path to Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
  6. In the window that opens, check the boxes to select the actions that should be scanned with the certificate installed. To view information about the certificate, click the **View** button.

- *To install the certificate for Mozilla Firefox version 3.x:*

  1. In the browser menu, select the **Tools** → **Settings** item.
  2. In the window that opens, select the **Additional** section.
  3. On the **Encryption** tab, click the **View Certificates** button.
  4. In the window that opens, select the **Authorities** tab and click the **Import** button.
  5. In the window that opens, select the Kaspersky Lab certificate file. The path to Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
  6. In the window that opens, check the boxes to select the actions that should be scanned with the certificate installed. To view information about the certificate, click the **View** button.

If your computer runs under Microsoft Windows Vista or Microsoft Windows 7, the path to Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

SCANNING ENCRYPTED CONNECTIONS IN OPERA

Opera browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Opera, you should install Kaspersky Lab's certificate manually.

- *To install the Kaspersky Lab certificate:*

  1. In the browser menu, select the **Tools** → **Settings** item.
  2. In the window that opens, select the **Additional** section.
  3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.
  4. In the window that opens, select the **Vendors** tab and click the **Import** button.

5. In the window that opens, select the Kaspersky Lab certificate file. The path to Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. In the window that opens, click the **Install** button. Kaspersky Lab's certificate is installed. To view information about the certificate, and to select actions for which the certificate will be used, select the certificate in the list and click the **View** button.

To install the Kaspersky Lab's certificate for Opera version 9.x:

1. In the browser menu, select the **Tools** → **Settings** item.

2. In the window that opens, select the **Additional** section.

3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.

4. In the window that opens, select the **Authorities** tab and click the **Import** button.

5. In the window that opens, select the Kaspersky Lab certificate file. The path to Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. In the window that opens, click the **Install** button. Kaspersky Lab's certificate is installed.

If your computer runs under Microsoft Windows Vista or Microsoft Windows 7, the path to Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

NETWORK MONITOR

Network Monitor is a tool used to view information about network activities in real time.

To start Network Monitor:

1. Open the main application window and select the **Protection Center** section.

2. In the right part of the window, left-click to open the **Online Security** list of components.

3. Click the **Network Monitor** link.

   Information about network activity is displayed in the **Network Monitor** window that opens.

When working on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can run Network Monitor using Kaspersky Gadget. To do this, Kaspersky Gadget should be configured so that the option of opening the Network Monitor window would be assigned to one of its buttons (see section "How to use Kaspersky Gadget" on page 72).

To run Network Monitor using Gadget,

click the button with the **Network Monitor** icon in the Kaspersky Gadget interface.

Information about network activity is displayed in the **Network Monitor** window that opens.

CONFIGURING THE PROXY SERVER

If the computer's Internet connection is established via a proxy server, you may need to edit its connection settings. Kaspersky Internet Security uses these settings for certain protection components, as well as for updating the databases and application modules.

If your network includes a proxy server using a non-standard port, you should add the port number to the list of monitored ports (see section "Creating a list of monitored ports" on page 131).

To configure the proxy server:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Network** component.
3. In the **Proxy server** section, click the **Proxy server settings** button.
4. In the **Proxy server settings** window that opens, modify the proxy server settings.

CREATING A LIST OF MONITORED PORTS

Such protection components as Mail Anti-Virus, Anti-Spam (see page 132), Web Anti-Virus (on page 100) and IM Anti-Virus monitor the data streams transferred via specific protocols and passing certain open TCP-ports on your computer. For example, Mail Anti-Virus scans information transferred via SMTP, while Web Anti-Virus scans information transferred via HTTP, HTTPS, and FTP.

You can enable monitoring all or just the selected network ports. If you configure the product to monitor the selected ports, you can specify the list of applications, for which all ports will be monitored. We recommend that you expand this list by including applications that receive or transfer data via FTP.

To add a port to the list of monitored ports:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Network** component.
3. In the **Monitored ports** section, select **Monitor selected ports only** and click the **Select** button.

   The **Network ports** window opens.
4. Click the **Add** link located under the list of ports in the top part of the window to open the **Network port** window, and enter the number and description of a port.

To exclude a port from the list of monitored ports:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Network** component.
3. In the **Monitored ports** section, select **Monitor selected ports only** and click the **Select** button.

   The **Network ports** window opens.
4. In the list of ports in the top part of the window, uncheck the box next to the description of the port that should be excluded.

To create the list of applications for which you wish to monitor all ports:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Network** component.
3. In the **Monitored ports** section, select **Monitor selected ports only** and click the **Select** button.

   The **Network ports** window opens.

4. Check the **Monitor all ports for specified applications** box and in the list of applications below check the boxes for the names of the applications for which all ports should be monitored.

5. If an application is not included in the list, add it as follows:

   a. To select a method for adding an application into the list, open the menu by clicking the **Add** link located under the list of applications, and select an item from the menu:

      - Select **Browse** to specify the location of the executable file. After you have selected the executable file, the **Application** window opens.

      - Select **Applications** to select an application from the list of currently active applications. After you have selected an application from the list, the **Application** window opens.

   b. In the **Application** window, enter the description for the application selected.

ANTI-SPAM

Kaspersky Internet Security includes *Anti-Spam*, a component that allows detection of unwanted messages (spam) and their processing in accordance with the rules in your e-mail client. It saves time while working with e-mail.

Anti-Spam is built into the following mail clients as a plug-in:

- Microsoft Office Outlook (on page 146);
- Microsoft Outlook Express (Windows Mail) (on page 146);
- The Bat! (on page 147);
- Thunderbird (on page 148).

You can use the lists of blocked and allowed senders to specify for Anti-Spam the addresses from which messages will be recognized as useful mail or spam. You may also assign the status of spam to the messages which are not addressed to you directly (see page 142). Furthermore, Anti-Spam can check a message for the presence of allowed and blocked phrases and also for phrases from the list of obscene expressions.

To enable efficient recognition of spam and useful mail by Anti-Spam, the component needs training (see section "Training Anti-Spam" on page 135).

Component operation algorithm

Anti-Spam uses a self-training algorithm that allows the component to tell spam from useful mail better with time. The source of data for the algorithm is the contents of the message.

Anti-Spam work consists of two stages:

1. Application of strict filtering criteria to a message. These criteria allow a quick determination as to whether the message is spam. Anti-Spam assigns to the message *spam* or *not spam* status, the scan is stopped and the message transferred to the mail client for processing (see algorithm steps 1 to 5 below).

2. Inspection of messages, which have passed strict selection criteria during previous steps. Such messages cannot be unambiguously considered spam. Therefore, Anti-Spam has to calculate for them the *probability* of being spam.

The Anti-Spam algorithm consists of the following steps:

1. The message sender's address is checked for its presence in the lists of allowed or blocked senders.

   - If a sender's address is in the allowed list, the message receives the *Not Spam* status.

- If a sender's address is in the black list, the message receives the *Spam* status.

2. If a message was sent using Microsoft Exchange Server and scan of such messages is disabled, the message is considered as *not spam*.

3. A message analysis is performed to check if it contains strings from the list of allowed phrases. If at least one line from this list has been found, the message will be assigned the *not spam* status. This step is skipped by default.

4. Anti-Spam analyzes a message to check if it contains strings from the list of blocked phrases or the list of obscene words. Whenever words from these lists are found in a message, their weighting coefficients are summed up. If the total of coefficients exceeds 100, such message will receive the *spam* status. This step is skipped by default.

5. If the message text contains an address included in the database of phishing or suspicious web addresses, the message receives the *Spam* status.

6. E-mail is analyzed using heuristic rules. If the analysis finds in a message signs typical of spam, the probability of it being spam increases.

7. E-mail is analyzed using the GSG technology. While doing it, Anti-Spam analyzes images attached to the email message. If the analysis finds in them signs typical of spam, the probability of the message being spam increases.

8. The application analyzes e-mail attachments in .rtf format. It scans attached documents checking them for the presence of spam signs. Once the analysis is complete, Anti-Spam calculates how much the probability of the message being spam increased. The technology is disabled by default.

9. It checks for the presence of the additional features typical of spam. Each detected feature increases the probability that the message being scanned is in fact spam.

10. If Anti-Spam was trained, the message will be scanned using iBayes technology. The self-training iBayes algorithm calculates the probability of a message being spam based on the frequency of phrases typical of spam found in message text.

Message analysis determines the probability of its being spam expressed as the *spam rate* value. The *Spam* or *Probable spam* status will be assigned to a message depending upon the specified threshold values of the spam rate (see section "Regulating threshold values of spam rate" on page 144). The product adds by default to the **Subject** field of spam and potential spam messages the label **[!! SPAM]** or **[!! Probable Spam]** (see section "**Adding a label to the message subject**" on page 145). Then each message will be processed in accordance with your rules defined for email clients (see section "Configuring spam processing by mail clients" on page 146).

IN THIS SECTION:

Enabling and disabling Anti-Spam 134

Selecting spam protection level 135

Training Anti-Spam 135

Scanning links in messages 138

Detecting spam by phrases and addresses. Creating lists 138

Regulating threshold values of spam rate 144

Using additional features affecting the spam rate 144

Selecting the spam recognition algorithm 144

Adding a label to the message subject 145

Excluding Microsoft Exchange Server messages from the scan 145

Configuring spam processing by mail clients 146

Restoring the recommended Anti-Spam settings 148

ENABLING AND DISABLING ANTI-SPAM

There are two ways to enable or disable the component:

- from the main application window (see section "Kaspersky Internet Security main window" on page 44);
- from the settings window (see section "Application settings window" on page 48).

To enable or disable Anti-Spam in the main window, perform the following steps:

1. Open the main application window and select the **Protection Center** section in the left part of the window.
2. In the right part of the window, left-click the **Online Security** or the **System and Applications Protection** section.
3. Open the menu for selecting an action on the component by clicking the **Anti-Spam** button and select **Enable Anti-Spam** (if the component should be enabled) or **Disable Anti-Spam** (if it should be disabled).

   When enabling a component, the icon on its left turns green and when disabling it, the icon turns grey.

To enable or disable Anti-Spam in the configuration window, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. In the right part of the window, check the **Enable Anti-Spam** box, if the component should be enabled. Uncheck the box if the component should be disabled.

SELECTING SPAM PROTECTION LEVEL

You can select the anti-spam protection level depending on the amount of spam arriving in your mailbox. The levels of anti-spam protection correspond to the following security levels configured by the experts at Kaspersky Lab:

- **High**. This security level should be used if you receive spam frequently; for example, while using free mail services. When you select this level, the frequency of false positives rises: that is, useful mail is more often recognized as spam.
- **Recommended**. This security level should be used in most cases.
- **Low**. This security level should be used if you rarely receive spam, for example, if you are working in a protected corporate email environment. When this level is selected, spam and potential spam messages are less frequently recognized.

To select one of the available security levels, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Use the slider in the right part of the window to choose the required security level.

   The name of the selected security level will appear below the **Security level** section header.

If none of the suggested security levels matches your requirements, you can configure Anti-Spam, for example, modify the threshold values for the spam rate or enable checks for Microsoft Exchange Server messages. Such configuration will change the security level name to **Custom**.

If you are not satisfied with the reconfigured behavior of Anti-Spam, you can restore the component configuration (see section "Restoring the recommended Anti-Spam settings" on page 148).

TRAINING ANTI-SPAM

One of the most powerful spam detection tools is the self-training iBayes algorithm. The application uses the algorithm to decide, which status should be assigned to a message based on the phrases it contains. Prior to work beginning, sample strings of useful and spam mail should be submitted to the iBayes algorithm, i.e. it should be *trained*.

There are several approaches to training Anti-Spam:

- Use the Training Wizard (packet training). Training with the Training Wizard is preferable from the very onset of using Anti-Spam.
- Training Anti-Spam using outgoing messages.
- Training is performed right while working with messages in mail client using the appropriate buttons and menu items.
- Training when working with Anti-Spam reports.

IN THIS SECTION:

Using the Training Wizard 136

Training Anti-Spam using outgoing messages. 136

Using mail client interface elements 137

Adding an address to the list of allowed senders 137

Training with reports 138

USING THE TRAINING WIZARD

The Training Wizard allows Anti-Spam training in batch mode. To do so, specify which folders of Microsoft Office Outlook or Microsoft Outlook Express (Windows Mail) accounts contain spam and which contain useful mail.

Correct spam recognition requires training using at least 50 samples of useful messages and 50 samples of unwanted mail. iBayes will not be operational until these steps are completed.

To save time, the Training Wizard only trains on 50 emails in each the selected folder.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

To start the Wizard:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Train** button in the **Anti-Spam training** section within the right part of the window.

While training using good mail, the application will automatically add addresses of the corresponding message senders to the list of allowed senders. You can disable the feature (see section "Adding an address to the list of allowed senders" on page 137).

TRAINING ANTI-SPAM USING OUTGOING MESSAGES.

You can train Anti-Spam using a sample of 50 outgoing emails. Once training is enabled, Anti-Spam will analyze every message you send using it as a sample of useful mail. Training will complete after you send the 50th message.

To enable Anti-Spam training on outgoing emails:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. On the **Additional** tab, in the **Outgoing messages** section check the **Train using outgoing email messages** box.

While training using outgoing mail is in progress, the addresses of mail recipients are automatically added to the list of allowed senders. You can disable the feature (see section "Adding an address to the list of allowed senders" on page 137).

USING MAIL CLIENT INTERFACE ELEMENTS

Training Anti-Spam while working directly with e-mail messages involves using special interface elements (toolbar buttons and menu items) of your mail client.

Please note that the buttons and menu items for Anti-Spam training only appear in the interfaces of mail client software after installation of Kaspersky Internet Security.

To train Anti-Spam using the email client:

1. Start the email client.
2. Select a message with which you wish to train Anti-Spam.
3. Please do the following depending upon your email client:
   - click the **Spam** or **Not Spam** button in the Microsoft Office Outlook toolbar;
   - click the **Spam** or **Not Spam** button in the Microsoft Outlook Express toolbar (Windows Mail);
   - use the special **Mark as Spam** and **Mark as Not Spam** items in the **Special** menu of The Bat! email client;
   - use the **Spam / Not Spam** button in the Mozilla Thunderbird toolbar.

After selecting an action from the list above, Anti-Spam performs training using the selected message. If you select several messages, all of them are used for training.

If a message is marked as useful mail, the address of its sender will be added to the list of allowed senders automatically. You can disable the feature (see section "Adding an address to the list of allowed senders" on page 137).

In cases when you need to immediately select several emails, or are certain that a folder contains emails of only one group (spam or not spam), you can take a multi-faceted approach to training using Training Wizard (see section "Training Anti-Spam" on page 135).

ADDING AN ADDRESS TO THE LIST OF ALLOWED SENDERS

When Anti-Spam is trained using regular mail in Training Wizard or directly in the mail client, the addresses of useful mail senders are automatically added to the list of allowed senders. The application also adds to that list the addresses of outgoing mail recipients if the component training with outgoing mail is used.

You can disable that functionality to prevent automatic addition of allowed senders to the list in the course of training.

To disable adding the address to the list of allowed senders:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. On the **Exact methods** tab, in the **Consider message as not spam** section, check the **If it is from an allowed sender** box and click the **Select** button.

   The **Allowed senders** window opens.
5. Uncheck the **Add allowed senders' addresses when training Anti-Spam** box.

TRAINING WITH REPORTS

There is an opportunity to train Anti-Spam using its reports with the information about messages recognized as probable spam. Essentially, the training means assigning the **Spam** or **Not Spam** labels to messages as well as adding them to the lists of allowed or blocked senders (see section "Blocked and allowed senders" on page 141).

To train Anti-Spam using a report:

1. Open the main application window.
2. Click the **Reports** link to switch to the reports window of Kaspersky Internet Security.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.

   The **Detailed report** window opens.
4. Select the **Anti-Spam** section in the left part of the window.
5. Use the records in the **Object** column in the right part of the window to identify the messages, which you wish to use for Anti-Spam training. For each such message, open the shortcut (right-click) menu and select one of the menu commands corresponding to the operation, which should be performed with the message:
   - Mark as Spam.
   - Mark as Not Spam.
   - Add to the allowed list.
   - Add to the blocked list.

SCANNING LINKS IN MESSAGES

Anti-Spam can check the URLs in mail messages to identify the ones included in the lists of suspicious web addresses or phishing web addresses. These lists are included into the product package of Kaspersky Internet Security. If a phishing or suspicious link is detected in a message, or if phishing elements are detected in the message body, this message is recognized as spam.

To enable URL checks using the databases of suspicious and phishing addresses:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. On the **Exact methods** tab, in the **Consider message as spam** section, check the **If it contains URLs from the database of suspicious URLs** and **If it contains phishing elements** boxes.

DETECTING SPAM BY PHRASES AND ADDRESSES. CREATING LISTS

You can create lists of allowed, blocked and obscene key phrases as well as lists of allowed and blocked sender addresses and the list of your addresses. If these lists are used, Anti-Spam analyzes every message to check if it contains the phrases added to the lists and the addresses of mail sender and recipients to check if they match the records in address lists. Once the sought phrase or address is found, Anti-Spam identifies such message as useful mail or spam depending upon the list where the phrase or address is present.

The following mail will be recognized as spam:

- messages containing blocked or obscene phrases with total weighting coefficient exceeding 100;
- messages sent from a blocked address or not addressed to you directly.

The following messages will be recognized as useful mail:

- messages containing allowed phrases;
- messages sent from an allowed address.

Masks for key phrases and sender addresses

You can use *phrase masks* in the lists of allowed, blocked and obscene phrases. The lists of allowed and blocked addresses, and the list of trusted addresses support *address masks*.

Mask is a template string that a phrase or an address is compared against. Certain symbols in a mask are used to represent others: ***** substitutes any sequence of characters, **?** – any single character. If a mask uses such wildcards, it can match several phrases or addresses (see examples).

If the ***** or **?** character is a part of the sought phrase (e.g., *What's the time?*), it should be preceded with the **** character to ensure that Anti-Spam recognizes it correctly. Thus, instead of the ***** character you should use in masks the ***** combination, the **?** character should be represented as **\?** (e.g., *What's the time**?*).

Sample phrase masks:

- *Visit our ** – this mask corresponds to a message that begins with the words *Visit our* and continues with any text.

Examples of address masks:

- *admin@test.com* – the mask only matches the address *admin@test.com*.
- *admin@** – the mask matches the sender address with the *admin* name, for example, *admin@test.com*, *admin@example.org.*
- **@test** – the mask matches the address of any message sender from a domain beginning with *test*, for example: *admin@test.com*, *info@test.org.*
- *info.*@test.???* – this mask corresponds to the address of any sender whose name begins with *info.* and whose mail domain name begins with *test.* and ends with any three characters, for example: *info.product@test.com*, *info.company@test.org*, not *info.product@test.ru*.

IN THIS SECTION:

Blocked and allowed phrases 140

Obscene words 140

Blocked and allowed senders 141

Your addresses 142

Exporting and importing lists of phrases and addresses 142

BLOCKED AND ALLOWED PHRASES

You can add to the list of *blocked phrases* the expressions, which you typically observe in spam, and define the weighting coefficient for each phrase. *Weighting coefficient* allows you to specify how typical a certain phrase can be for spam messages: the larger the value, the higher the probability that mail containing such phrase is spam. Weighting coefficient of a phrase can range from 0 to 100. If the total of weighting coefficients of all phrases found in a message exceeds 100, such mail will be recognized as spam.

Key expressions typical of useful mail can be added to the list of *allowed phrases*. Once Anti-Spam finds such phrase in a message, it will be identified as useful mail (not spam).

You can add both entire phrases and their masks to the lists of blocked and allowed phrases (see section "Detecting spam by phrases and addresses. Creating lists" on page 138).

To create the list of blocked or allowed phrases:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. Use the **Exact methods** tab to perform the following steps:

   - If you need to create a list of blocked phrases, in the **Consider message as spam** section, check the **If it contains blocked phrases** box and click the **Select** button to the right.

     The **Blocked phrases** window will open.
   - If you need to create a list of allowed phrases, in the **Consider message as not spam** section, check the **If it contains allowed phrases** box and click the **Select** button to the right.

     The **Allowed phrases** window will open.
5. Click the **Add** link to open the **Blocked phrase** window (or the **Allowed phrase** window).
6. Enter the complete phrase or expression mask, specify the weighting coefficient for a blocked phrase and then click **OK**.

You do not have to delete a mask to stop using it, unchecking the corresponding box next to it will be sufficient for the purpose.

OBSCENE WORDS

Kaspersky Lab experts have compiled the list of obscene words included into the distribution package of Kaspersky Internet Security. The list contains obscene words that indicate a spam message with high probability, if present. You can supplement the list, adding complete phrases and their masks to it (see section "Detecting spam by phrases and addresses. Creating lists" on page 138).

If Parental Control (see page 156) is enabled for the user and a password (see page 76) for editing the Parental Control settings is set, the user should enter the password to view the list of obscene phrases.

To edit the list of obscene phrases:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.

3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.

4. On the **Exact methods** tab, in the **Consider message as spam** section check the **If it contains blocked phrases** box and click the **Select** button.

   The **Blocked phrases** window will open.

5. Check the **Consider as blocked obscene words** box and click the **obscene words** link to open the **Agreement** dialog.

6. Read the agreement and, if you agree to the terms and conditions described in the window, check the box in the bottom part of the window and click the **OK** button.

   The **Explicit language** window will open.

7. Click the **Add** link to open the **Blocked phrase** window.

8. Enter the complete phrase or its mask, specify the phrase weighting coefficient and click **OK**.

You do not have to delete a mask to stop using it, unchecking the **Explicit language** box next to it will be sufficient for the purpose.

BLOCKED AND ALLOWED SENDERS

You can add to the list of *blocked senders* the addresses, mail from which Anti-Spam will recognize as spam. Sender addresses from which you expect no spam are stored in the list of *allowed senders*. The list is created automatically during Anti-Spam training (see section "Adding an address to the list of allowed senders" on page 137). You can also supplement the list manually.

You can add to the lists of allowed or blocked senders complete addresses or address masks (see section "Detecting spam by phrases and addresses. Creating lists" on page 138).

To create the list of blocked or allowed senders:

1. Open the application settings window.

2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.

3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.

4. Use the **Exact methods** tab to perform the following steps:

   - If you need to create a list of blocked senders, in the **Consider message as spam** section, check the **If it is from a blocked sender** box and click the **Select** button to the right.

     The **Blocked senders** window will open.

   - If you need to create a list of allowed senders, in the **Consider message as not spam** section, check the **If it is from an allowed sender** box and click the **Select** button to the right.

     The **Allowed senders** window opens.

5. Click the **Add** link to open the **Email address mask** window.

6. Enter an address mask and click the **OK** button.

You do not have to delete a mask to stop using it, unchecking the corresponding box next to it will be sufficient for the purpose.

YOUR ADDRESSES

You can create a list of your mail addresses to make Anti-Spam label as spam any mail that is not addressed to you directly.

To create the list of your email addresses:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. On the **Exact methods** tab, check the **If it is not addressed to me** box and click the **My addresses** button.

   The **My addresses** window opens.
5. Click the **Add** link to open the **Email address mask** window.
6. Enter an address mask and click the **OK** button.

You do not have to delete a mask to stop using it, unchecking the corresponding box next to it in **My addresses** window will be sufficient for the purpose.

EXPORTING AND IMPORTING LISTS OF PHRASES AND ADDRESSES

Having created the lists of phrases and addresses, you can reuse them, for example, transfer the addresses to a similar list on another computer running Kaspersky Internet Security.

To do this:

1. Make *export* – copy records from the list into a file.
2. Move the file you have saved to another computer (for example, send it by email or use a removable data medium).
3. Make *import* – add the records from the file to the list of the same type on another computer.

While exporting the list, you can copy either the selected list element only, or the entire list. While importing the list, you can add the new elements to the existing list, or replace the existing list with the one being imported.

To export records from a list, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. On the **Exact methods** tab, check the box in the line containing the name of the list where the records should be exported, and click the corresponding button to the right.
5. Use the displayed list window to check the records, which should be included into the file.
6. Click the **Export** link.

This action opens a window that offers you to export the highlighted items only. In this window, take one of the following actions:

- click the **Yes** button if you need to include only selected records in the file;
- click the **No** button if you need to include the entire list in the file.

7. Specify in the displayed window the type and name for the file and confirm its saving.

To import records from file to a list, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. On the **Exact methods** tab check the box in the line containing the name of the list where the records should be imported, and click the button to the right.
5. Click the **Import** link in the list window. If you are importing a list of allowed senders, the application will display a menu where you should select the **Import from file** item. For other list types selection from the menu is not required.

   If the list is not empty, a window opens offering you to add items to be imported. In this window, take one of the following actions:

   - click the **Yes** button if you want to add records from the file into the list;
   - click the **No** button if you want to replace the existing records with the list from the file.
6. In the window that opens, select the file with the list of records that you want to import.

Importing the list of allowed senders from address book

Addresses in the list of allowed senders can be imported from Microsoft Office Outlook / Microsoft Outlook Express (Windows Mail) address books.

To import the list of allowed senders from an address book, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. On the **Exact methods** tab, in the **Consider message as not spam** section, check the **If it is from an allowed sender** box and click the **Select** button.

   The **Allowed senders** window opens.
5. Click the **Import** link, open the source selection menu, and select **Import from the Address Book**.
6. Use the displayed window to select the necessary address book.

REGULATING THRESHOLD VALUES OF SPAM RATE

Spam recognition is based on cutting-edge filtering methods, which allow you to train (see section "Training Anti-Spam" on page 135) Anti-Spam to distinguish spam, probable spam and useful email. In doing so, every individual element of good emails or spam is assigned a factor.

When an email message enters your inbox, Anti-Spam scans the message using the iBayes algorithm for elements of spam and good email. The component sums up the ratings of each spam (useful mail) item and calculates the resulting *spam rate*. The larger the spam rate, the higher the probability that such mail contains spam. A message is recognized by default as useful mail if its spam rate does not exceed 60. If spam rate is higher than 60, such message is considered to be potential spam. If the value exceeds 90, such message is recognized as spam. You can modify the threshold values for the spam rate.

To change the spam rate thresholds, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. On the **Expert methods** tab, use the **Spam rate** section to configure the spam rate values using the corresponding sliders or entry fields.

USING ADDITIONAL FEATURES AFFECTING THE SPAM RATE

The result of spam rate calculation can be affected by additional message characteristics, for example, a missing recipient's address in the "To" field or a very long message subject (over 250 characters). When present in a message, such signs increase the probability of its being spam. Consequently, the spam rate will grow. You can select the additional signs that will be taken into account during message analysis.

To use additional signs increasing the spam rate, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. On the **Expert methods** tab, click the **Additional** button.
5. In the displayed **Additional** window, check the boxes ☑ next to the signs, which should be taken into account during message analysis increasing the spam rate.

SELECTING THE SPAM RECOGNITION ALGORITHM

The Anti-Spam mail analysis is based on the selected recognition algorithms:

- **Heuristic Analysis**. Anti-Spam analyzes messages using heuristic rules. Heuristic analysis is always enabled.
- **Image recognition (GSG technology)**. Anti-Spam uses GSG technology to detect graphic spam.
- **Analysis of attachments in RTF format**. Anti-Spam analyzes documents attached to messages checking them for spam signs.

- **Self-training text recognition algorithm (iBayes)**. Operation of the iBayes algorithm is based on the analysis calculating the frequency of words typical for spam in the text of the analyzed mail. The analysis identifies each message as useful mail or spam. To start using the iBayes algorithm, you should train Anti-Spam (see section "Training Anti-Spam" on page 135).

To enable / disable a specific spam recognition algorithm for analysis of email messages:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. On the **Expert methods** tab, in the **Recognition algorithms** section check / uncheck the appropriate boxes.

ADDING A LABEL TO THE MESSAGE SUBJECT

Anti-Spam can add appropriate labels to the **Subject** field of the message recognized after analysis as spam or potential spam:

- **[!! SPAM]** – for messages identified as spam.
- **[?? Probable Spam]** – for messages identified as potential spam.

When present in message subject, such labels can help you distinguish spam and probable spam visually while viewing the mail lists.

To enable / disable addition of labels to the message subjects by Anti-Spam:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.
4. Use the **Additional** tab to select in the **Actions** section the checkboxes ☑ next to the labels, which should be added to message subject. Having checked the box, you can modify the associated label text. To prevent label addition, uncheck its corresponding box.

EXCLUDING MICROSOFT EXCHANGE SERVER MESSAGES FROM THE SCAN

You can exclude from anti-spam scanning email messages which originate within the internal network (for example, corporate mail). Please note that messages are considered internal mail if Microsoft Office Outlook is used on all network computers and user mailboxes are located on the same Exchange server or on servers linked via X400 connectors.

By default, the Anti-Spam component does not scan Microsoft Exchange Server messages.

If you wish Anti-Spam to analyze the messages transferred via Microsoft Exchange Server, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.

3. Click the **Settings** button in the right part of the window.

   The **Anti-Spam** window will be displayed.

4. On the **Additional** tab, in the **Exclusions** section uncheck the **Do not check Microsoft Exchange Server native messages** box.

CONFIGURING SPAM PROCESSING BY MAIL CLIENTS

If after scanning you find that an email is spam or probable spam, further actions of Anti-Spam depend on the status of the message and the action selected. By default, email messages considered spam or probable spam, are modified: in the **Subject** field of the message, the label **[!! SPAM]** or **[?? Probable Spam]** is added, respectively (see section "Adding a label to the message subject" on page 145).

You can select additional actions to be taken on spam or probable spam. To do so, special plug-ins are provided in the Microsoft Office Outlook and Microsoft Outlook Express (Windows Mail) clients. You can configure filtration rules for The Bat! and Thunderbird email clients.

IN THIS SECTION:

Microsoft Office Outlook 146

Microsoft Outlook Express (Windows Mail) 146

Creating the rule for handling spam reports 146

The Bat! 147

Thunderbird. 148

MICROSOFT OFFICE OUTLOOK

By default, email messages classified by Anti-Spam as spam or probable spam are marked with special labels **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** field. If additional mail processing after Anti-Spam checks is required, you can configure Microsoft Office Outlook as necessary. The spam processing settings window automatically opens the first time you run Microsoft Outlook after installing Kaspersky Internet Security. The spam and probable spam processing settings for Microsoft Outlook are displayed on the special **Anti-Spam** tab of the **Tools** → **Options** menu item.

MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

By default, email messages classified by Anti-Spam as spam or probable spam are marked with special labels **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** field. If additional mail processing after Anti-Spam checks is required, you can configure Microsoft Outlook Express (Windows Mail) as necessary.

The spam processing settings window opens when you run your client after the installation of the application. You can also open it by clicking the **Settings** button in the e-mail client toolbar next to the **Spam** and **Not Spam** buttons.

CREATING THE RULE FOR HANDLING SPAM REPORTS

Below are the instructions for creating the rule for handling spam reports using Anti-Spam in Microsoft Office Outlook. You can use the guidelines to create custom rules.

To create a spam processing rule:

1. Run Microsoft Office Outlook and use the **Tools** → **Rules and Alerts** command in the main application menu. The method used to access the wizard depends upon your version of Microsoft Office Outlook. This Help file describes how to create a rule using Microsoft Office Outlook 2003.

2. In the **Rules and Alerts** window that opens, on the **Email Rules** tab click the **New Rule** button. As a result, the Rules Wizard is launched. The Rules Wizard includes the following steps:

   a. You should decide whether you want to create a rule from scratch or use a template. Select the **Start from a blank rule** option and select the **Check messages when they arrive** scan condition. Click the **Next** button.

   b. Click the **Next** button in the message filtering condition configuration window without checking any boxes. Confirm in the dialog box that you want to apply this rule to all emails received.

   c. In the window for selecting actions in respect to messages, check the **perform a custom action** box in the action list. In the lower part of the window, click the **a custom action** link. Select **Kaspersky Anti-Spam** from the drop-down list in the window that opens and click the **OK** button.

   d. Click the **Next** button in the exclusions from the rules window without checking any boxes.

   e. In the final window, you can change the rule's name (the default name is Kaspersky Anti-Spam). Make sure that the **Turn on this rule** box is checked, and click the **Finish** button.

3. The default position for the new rule is first on the rule list in the **Rules and Alerts** window. If you like, move this rule to the end of the list so it is applied to the email last.

All incoming emails are processed with these rules. The order in which rules are applied depends upon the priority specified for each rule. Rules are applied from the list beginning; the priority of each following rule is lower than that of the preceding one. You can increase or decrease rule priority moving a rule up or down in the list. If you do not want the Anti-Spam rule to further process emails after a rule is applied, you must check the **Stop processing more rules** box in the rule settings (see Step 3 in creating a rule).

THE BAT!

Actions in respect of spam and probable spam in The Bat! are defined by the client's own tools.

To modify spam processing rules in The Bat!:

1. In the **Settings** item from the **Properties** menu of the mail client.

2. Select the **Spam protection** object from the settings tree.

Displayed settings of anti-spam protection apply to all installed Anti-Spam modules that support integration with The Bat!.

You need to define the rating level and specify how messages with certain a rating should be handled (in case of Anti-Spam – the probability of message being spam):

- delete messages with the rating that exceeds the specified value;
- move email messages with a given rating to a special spam folder;
- move spam marked with special headers to the spam folder;
- leave spam in the **Inbox** folder.

After processing an email, Kaspersky Internet Security assigns a spam or probable spam status to the message based on a rating with an adjustable value. The Bat! has its own email rating algorithm for spam, also based on a spam rate. To prevent discrepancies between spam rate in Kaspersky Internet Security and The Bat!, all messages checked in Anti-Spam are assigned the rating corresponding to the message status: Not Spam email – 0%, Probable spam – 50%,

Spam – 100%. Thus, the email rating in The Bat! corresponds to the rating of the relevant status and not to the spam rate assigned in Anti-Spam.

For more details on the spam rate and processing rules, see documentation for The Bat!.

THUNDERBIRD

By default, email messages classified by Anti-Spam as spam or probable spam are marked with special labels **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** field. If additional mail processing after Anti-Spam checks is required, you can configure Thunderbird having opened its configuration window from the **Tools** → **Message Filters** menu (for more details about using the mail client see Mozilla Thunderbird Help).

Thunderbird's Anti-Spam plug-in module allows training based on messages received and sent using this email client application and checking your email correspondence for spam on the server. The plug-in module is integrated into Thunderbird and forwards messages to the Anti-Spam component for scanning when commands from the **Tools** → **Run anti-spam filters** in folder menu are being executed. As such, Kaspersky Internet Security checks messages instead of Thunderbird. This does not alter the functionality of Thunderbird.

The Anti-Spam plug-in module status is displayed as an icon in the Thunderbird status line. The gray color of the icon informs the use that there is a problem in the plug-in operation or that the Anti-Spam component is disabled. Double-click the icon to open the settings of Kaspersky Internet Security. To modify the Anti-Spam settings, click the **Settings** button in the **Anti-Spam** section.

RESTORING THE RECOMMENDED ANTI-SPAM SETTINGS

If you are not satisfied with the reconfigured behavior of Anti-Spam, you can restore the component configuration advised by Kaspersky Lab and combined in the **Recommended** security level.

To restore default Anti-Spam settings:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
3. Click the **Default level** button in the **Security level** section in the right part of the window.

   Security level will be set to **Recommended**.

ANTI-BANNER

Anti-Banner is designed to block banners on web pages you open and those in the interface of specified applications. Ads on banners may distract you from your business activity while banner downloads increase the amount of inbound traffic.

Before a banner is displayed on a web page or in an application's window, it should be downloaded from the Internet. Anti-Banner scans the address from which the banner is downloaded. If the address is associated to a mask from the list included with the Kaspersky Internet Security package, or from the list of blocked banners addresses you have compiled on your own, Anti-Banner blocks the banner. To block banners with address masks not found in the mentioned lists, the heuristic analyzer is used (see section "Selecting the scan method" on page 149).

Additionally, you can create a list of allowed addresses to determine which banners should be allowed for display.

IN THIS SECTION:

Enabling and disabling Anti-Banner 149

Selecting the scan method 149

Creating the lists of blocked and allowed banner addresses 150

Exporting and importing the lists of addresses 150

ENABLING AND DISABLING ANTI-BANNER

Immediately after Kaspersky Internet Security installation the Anti-Banner component is disabled, it does not block banners. To activate banner blocking, you have to enable the Anti-Banner.

To display all banners, the Anti-Banner component should be disabled. If you need to display just some banners, use the list of allowed banner addresses (see section "Creating the lists of blocked and allowed banner addresses" on page 150).

There are two ways to enable or disable the component:

- from the main application window (see section "Kaspersky Internet Security main window" on page 44);
- from the settings window (see section "Application settings window" on page 48).

To enable or disable Anti-Banner in the main window, perform the following steps:

1. Open the main application window and select the **Protection Center** section in the left part of the window.
2. In the right part of the window, left-click to open the **Online Security** section.
3. Click the **Anti-Banner** button to open the menu for selecting actions on the component and select **Enable Anti-Banner** (if the component should be enabled) or **Disable Anti-Banner** (if it should be disabled).

   When enabling a component, the icon on its left turns green and when disabling it, the icon turns grey.

To enable or disable Anti-Banner in the configuration window, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Banner** component.
3. In the right part of the window, check the **Enable Anti-Banner** box, if the component should be enabled. Uncheck the box if the component should be disabled.

SELECTING THE SCAN METHOD

You can specify which methods should be used by Anti-Banner to scan addresses from which banners may be downloaded. In addition to these methods, Anti-Banner checks banner addresses for compliance to the masks from the lists of allowed and blocked addresses if those are in use.

To select methods of address scan by Anti-Banner:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Banner** component.
3. In the right part of the window, in the **Scan methods** group, check the boxes next to the names of the methods that should be used.

CREATING THE LISTS OF BLOCKED AND ALLOWED BANNER ADDRESSES

Using the lists of blocked and allowed banners addresses, you can allow banners to be downloaded for a specified group of addresses and block them for another group. Create a list of blocked address masks to let Anti-Banner block download and display of banners from the addresses that correspond to those masks. Create a list of allowed address masks to let Anti-Banner download and display banners from the addresses that correspond to those masks.

To add a mask to the list of blocked (allowed) addresses:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Banner** component.
3. In the right part of the window, in the **Additional** section, check the **Use the list of blocked URLs** box (or the **Use the list of allowed URLs** box) and click the **Settings** button located under the box.

   The **Blocked URLs** (or **Allowed URLs**) window opens.
4. Click the **Add** button.

   The **Address mask (URL)** window will open.
5. Enter a blocked (or allowed) banner mask and click the **OK** button.

You do not have to delete a mask to stop using it, unchecking the corresponding box next to it will be sufficient for the purpose.

EXPORTING AND IMPORTING THE LISTS OF ADDRESSES

After you have created the lists of allowed or blocked banner addresses, you can use them repeatedly: for example, export banner addresses to a similar list on another computer with Kaspersky Internet Security installed on it.

To do this:

1. Make *export* – copy records from the list into a file.
2. Move the file you have saved to another computer (for example, send it by email or use a removable data medium).
3. Make *import* – add the records from the file to the list of the same type on another computer.

While exporting the list, you can copy either the selected list element only, or the entire list. While importing the list, you can add the new elements to the existing list, or replace the existing list with the one being imported.

To export banner addresses from the list of allowed or blocked URLs, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Banner** component.
3. In the right part of the window, in the **Additional** section, click the **Settings** button located in the line with the name of the list from which you should copy addresses into a file.
4. In the **Allowed URLs** (or **Blocked URLs**) window that opens, check the boxes next to the addresses that you need to include in the file.
5. Click the **Export** button.

This action opens a window that offers you to export the highlighted items only. In this window, take one of the following actions:

- click the **Yes** button if you need to include only selected addresses in the file;
- click the **No** button if you need to include the entire list in the file.

6. In the window that opens, enter a name for the file you want to save and confirm saving.

To import banner addresses from a file to the list of allowed or blocked URLs, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Anti-Banner** component.
3. In the right part of the window, in the **Additional** section, click the **Settings** button located in the line with the name of the list into which you need to add addresses from a file.
4. In the **Allowed URLs** window (or the **Blocked URLs** window) that opens, click the **Import** button.

   If the list is not empty, a window opens offering you to add items to be imported. In this window, take one of the following actions:

   - click the **Yes** button if you want to add records from the file into the list;
   - click the **No** button if you want to replace the existing records with the list from the file.
5. In the window that opens, select the file with the list of records that you want to import.

SAFE RUN

Safe Run is a secure environment isolated from the main operating system and designed for running applications whose safety raises doubts as well as for working with online banking resources when security of confidential data has a great importance. When you use Safe Run, the real objects of the operating system do not undergo changes. So even if you run an infected application in Safe Run, all of its actions will be limited to the virtual environment without affecting the operating system.

In the current version of Kaspersky Internet Security, Safe Run offers the following functionality:

- Safe Run for Applications (see section "Starting and ending operations in Safe Run for Applications" on page 153);
- running an individual application in Safe Run (on page 152);
- Safe Run for Websites (on page 155);
- Virtual Keyboard (on page 62).

Suspicious objects detected while you work in the safe environment are quarantined in the normal mode. The type of safe environment and the original file locations are saved in the list of detected threats and in the full report of Kaspersky Internet Security. When objects are recovered from Quarantine, they are restored to the original folder. If the original folder cannot be found, Kaspersky Internet Security offers you to specify a location to restore the object in the environment in which the restoration procedure has been started.

Safe Run is not available on computers running Microsoft Windows XP x64.

The functionality of certain applications launched on computers running Microsoft Windows Vista x64 and Microsoft Windows 7 x64 is limited when operating in the safe environment. If such applications are started, the corresponding message is displayed on screen if you have enabled notifications of the **Application functionality is limited in safe mode** event. In addition, Safe Run for Applications is completely inaccessible.

IN THIS SECTION:

Safe Run for Applications 152

Safe Run for Websites 155

SAFE RUN FOR APPLICATIONS

It is recommended to use the safe environment for launching suspicious applications as well as trusted applications the vulnerabilities of which can be exploited by criminals to access data on your computer.

You can run an application (see section "Running an application in Safe Run" on page 152) in the safe environment as well as use the safe desktop (see section "Starting and stopping Safe Run for Applications" on page 153).

Safe Run for Applications opens in the full-screen mode and represents a copy of the main desktop with all file system objects.

You can create a list of applications that will run automatically when you start Safe Run for Applications.

By default, after you close Safe Run for Applications, all changes you have made during the last session will be saved and remain available at the next startup. If necessary, you can clear all changes (see page 155) made to the safe environment.

IN THIS SECTION:

Running an application in Safe Run 152

Starting and ending operations in Safe Run for Applications 153

Switching between the main desktop and Safe Run for Applications 153

Using the pop-up toolbar 154

Automatic running of applications 154

Using a shared folder 154

Clearing Safe Run for Applications 155

RUNNING AN APPLICATION IN SAFE RUN

You can run applications in Safe Run, without switching to the safe desktop. You can run an application in Safe Run from the context menu of Microsoft Windows.

Applications running in safe environment, are highlighted with a green frame around the application window, and have a safe run indicator in the list of applications monitored by Application Control (see section "Application Control" on page 113).

After the application is closed, all changes made by this application will be cleared.

- *To run an application in safe environment from the Microsoft Windows context menu,*

  right-click to open the context menu for the selected object (shortcut or executable file of the application) and select **Safe Run**.

STARTING AND ENDING OPERATIONS IN SAFE RUN FOR APPLICATIONS

Safe Run for Applications can be started by the following means:

- from the Kaspersky Internet Security main window (see section "Kaspersky Internet Security main window" on page 44);
- from the Kaspersky Internet Security context menu (see section "Context menu" on page 43);
- using a button in the Kaspersky Gadget interface if the option of running Safe Run for Applications is assigned to the button (see section "How to use Kaspersky Gadget" on page 72).

Safe Run can be closed from the **Start** menu of the operating system, from the pop-up toolbar (see section "Using the pop-up toolbar" on page 154), or using the key combination **ALT+SHIFT+CTRL+K**.

To start Safe Run for Applications from the main Kaspersky Internet Security window:

1. Open the main application window and select the **Safe Run** section.
2. Select **Safe Run for Applications** in the right part of the window.

To start Safe Run for Applications from the Kaspersky Internet Security context menu,

right-click to open the context menu on the Kaspersky Internet Security icon in the notification area and select **Safe Run for Applications**.

To start Safe Run for Applications from Kaspersky Gadget,

click the button with the **Safe Run for Applications** icon in the Kaspersky Gadget interface (only for Microsoft Windows Vista and Microsoft Windows 7).

To close Safe Run from the Start menu,

in the **Safe Run for Applications – shutdown** in the **Start** menu of the operating system.

To close Safe Run from the pop-up toolbar:

1. Roll over the top part of the screen with the mouse pointer.
2. In the pop-up toolbar, click the button.
3. In the selecting action window that opens, select **Disable**.

SWITCHING BETWEEN THE MAIN DESKTOP AND SAFE RUN FOR APPLICATIONS

You can switch to the main desktop, without closing Safe Run, and then switch back. You can use the following methods to switch between the main desktop and the Safe Run:

- from the Kaspersky Internet Security main window (see section "Kaspersky Internet Security main window" on page 44);
- from the Kaspersky Internet Security context menu (see section "Context menu" on page 43);
- from the pop-up toolbar (see section "Using the pop-up toolbar" on page 154) (available in Safe Run only);
- using the gadget (see section "Kaspersky Gadget" on page 49).

To switch to the main desktop from the main window of Kaspersky Internet Security:

1. Open the main application window and select the **Safe Run** section.
2. In the right part of the window, select **Main desktop**.

To switch to the main desktop from the context menu of Kaspersky Internet Security,

right-click to open the context menu on the Kaspersky Internet Security icon in the notification area and select **To the main**.

To switch to the main desktop from the pop-up toolbar:

1. Roll over the top part of the screen with the mouse pointer.
2. In the pop-up toolbar, click the button.

USING THE POP-UP TOOLBAR

Safe Run pop-up toolbar allows you to perform the following actions:

- close Safe Run for Applications (see section "Starting and shutting down Safe Run for Applications" on page 153);
- switch to the main desktop (see section "Switching between the main desktop and Safe Run for Applications" on page 153).

To display the pop-up toolbar in Safe Run,

roll over the top part of the screen with the mouse pointer.

To fix the pop-up toolbar:

1. Roll over the top part of the screen with the mouse pointer.
2. In the pop-up toolbar, click the button.

AUTOMATIC RUNNING OF APPLICATIONS

You can create a list of applications that will run automatically when you start Safe Run for Applications.

The autorun list can be generated only when Safe Run is enabled.

To generate the autorun list for Safe Run for Applications:

1. In the **Start** menu of the operating system, select **Programs** → **Autorun** → **Safe Run for Applications**.
2. Right-click to open the context menu and select **Open**.
3. Copy applications icons to be launched by the start of Safe Run for Applications into the opened folder.

USING A SHARED FOLDER

Shared folder of Safe Run is designed to share files between the main operating system and safe environment. All files saved in this folder when working in safe environment are available from the standard desktop.

Shared folder is created when the application is being installed. Location of the shared folder may vary depending on the operating system:

- for Microsoft Windows XP – c:\Documents and Settings\All Users\Application Data\Kaspersky Lab\SandboxShared;
- for Microsoft Windows Vista and Microsoft Windows 7 – c:\ProgramData\Kaspersky Lab\SandboxShared.

Location of the shared folder cannot be changed.

The safe environment shared folder can be opened in two ways:

- from the main application window (see section "Kaspersky Internet Security main window" on page 44);
- in the My Computer section of the Microsoft Windows Explorer (the shared folder's icon is).

To open the shared folder from the Kaspersky Internet Security's main window:

1. Open the main application window and select the **Safe Run** section.
2. Open the Safe Run shared folder in the standard window of Microsoft Windows by clicking the **Shared Folder** link in the right part of the window in the **Safe Run for Applications** section.

CLEARING SAFE RUN FOR APPLICATIONS

If you need to delete data saved when working in the safe application launch environment, and restore the modified settings, you can clear Safe Run for Applications.

The clearing is carried out from the main Kaspersky Internet Security window on the main desktop and only if the safe application launch is disabled.

Prior to emptying make sure that all data that may be needed for further work were saved in the Safe Run shared folder. Otherwise, the data is deleted without any possibility to restore them.

To clear Safe Run data:

1. Open the main application window and select the **Safe Run** section.
2. Click the **Clear** link in the right part of the window in the **Safe Run for Applications** section.

SAFE RUN FOR WEBSITES

The Safe Run for Websites is mainly designed for accessing online banking systems and other websites processing confidential data.

You can enable controlled access to online banking services (see section "Controlling access to online banking services" on page 106) to automatically detect banking websites as well as create your own list of websites; attempting to access them, you will be suggested to switch to Safe Run for Websites. Additionally, you can start Safe Run for Websites manually (see section "Starting Safe Run for Websites" on page 156).

When you use Safe Run for Websites, all changes (saved cookies, log of visited websites, etc.) remain in the safe environment and do not affect the operating system, which means that they cannot be exploited by intruders. If necessary, you can clear all changes (see section "Clearing the browser after viewing websites in safe mode" on page 156) made to the safe browser and restore the default settings.

Additionally, when working in Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome, Kaspersky Internet Security can automatically detect attempts to go to unknown or potentially dangerous websites and offer you to run your browser in the safe environment in order to preserve the operating system from probable risks caused by unknown web resources that you may have visited.

To ensure automatic detection of unknown websites, Safe Surf (see page 105) of Web Anti-Virus should be enabled.

IN THIS SECTION:

Starting Safe Run for Websites 156

Clearing the browser after viewing websites in safe mode 156

STARTING SAFE RUN FOR WEBSITES

When starting Safe Run for Websites, the default browser opens in Safe Run mode (only for Microsoft Internet Explorer, Mozilla Firefox, Google Chrome; in other cases, Microsoft Internet Explorer opens in Safe Run for Websites mode).

The browser which runs in Safe Run for Websites mode is highlighted with a green frame around the application window.

To start Safe Run for Websites from the Kaspersky Internet Security main window:

1. Open the main application window and select the **Safe Run** section.
2. In the right part of the window, select **Safe Run for Websites**.

CLEARING THE BROWSER AFTER VIEWING WEBSITES IN SAFE MODE

If you need to delete the data that have been saved when viewing websites in Safe Run, you can clear the safe browser.

To clear the Safe Run for Websites data:

1. Open the main application window and select the **Safe Run** section.
2. In the right part of the window, click the **Clear** link in the **Safe Run for Websites** section.

PARENTAL CONTROL

Parental Control allows the control of actions of users taken on the computer and on the network. The concept of control provides the option to restrict access to resources and applications as well as view reports of users' activities.

Nowadays, an ever-increasing number of children and teenagers obtain access to computers and web resources. This means problems for security since activity and communication on the Internet may entail a whole range of threats. These are the most frequent ones:

- access to websites that could waste time (chat rooms, games) or money (e-stores, auctions);
- access to websites targeted at the adult audience, such as those handling porn, extremism, firearms, drug abuse, and explicit violence;
- download of files infected with malware;
- excessive time of computer use, which may result in health deterioration;
- contacts with unfamiliar people which may pretend to be peers to obtain privacy information from the user, such as real name, physical address, time of day when nobody is home.

Parental Control allows you to reduce risks posed by the computer and the Internet. To do this, the following module's functions are used:

- limiting the time of computer and Internet use;
- creating lists of allowed and blocked applications as well as temporarily limiting number of startups for allowed applications;
- creating lists of allowed and blocked websites, specifying categories of websites with content not recommended for viewing;
- enabling the safe search mode involving search engines (links to websites with suspicious content are not displayed in the search results);
- restricting file downloads from the Internet;
- creating lists of contacts which are allowed or blocked for communication via IM clients and social networks;
- viewing message logs from IM clients and social networks;
- blocking sending of specified privacy data;
- searching for specified key words in message logs.

All these restrictions can be enabled independently from each other, which allows you to flexibly configure Parental Control for various users. For each account, you can view reports which contain events for the categories being controlled that the component has logged over the specified period.

To start managing the component, you should go through an authentication procedure by entering the administrator name and password (see section "Restricting access to Kaspersky Internet Security" on page 76). If you have not yet set a password for managing Kaspersky Internet Security, you will be offered to do this.

IN THIS SECTION:

Configuring user's Parental Control 157

Viewing reports of user's activity 165

CONFIGURING USER'S PARENTAL CONTROL

You can enable and configure Parental Control for each account separately, by imposing different limits on different users, such as age limits. You can also disable Parental Control for the users whose activity needs no control.

IN THIS SECTION:

Enabling and disabling user's control 158

Exporting and importing Parental Control settings 159

Displaying an account in Kaspersky Internet Security 160

Time of computer use 160

Running applications 161

Time of Internet use 161

Viewing websites 161

Downloading files from the Internet 162

Communicating via IM clients 162

Communicating via social networks 164

Sending confidential information 164

Searching for key words 165

ENABLING AND DISABLING USER'S CONTROL

You can enable and disable Parental Control individually for every account. E.g., there is no need to control the activity of an adult user of the administrator account – Parental Control for this can be disabled. For other users whose activity should be controlled, the Parental Control should be enabled and configured, for example, by loading the standard configuration from a template.

You can enable or disable Parental Control for any account using the following methods:

- from the main application window;
- from the **Parental Control** window;
- from the Parental Control settings window;

You can enable or disable Parental Control for the current account using the context menu of the application icon.

To enable or disable Parental Control for an account from the main window, perform the following steps:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, in the section with the user account, click the button if you want to enable Parental Control for the selected account. If you want to disable Parental Control, click the button .

To enable or disable Parental Control for an account from the Parental Control window:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user for whom you want to enable or disable Parental Control.

   The **Parental Control** window opens.

3. Open the **Settings** tab and select the **User Account Settings** section in the left part of the window.

4. In the right part of the window, check the **Enable control for the user** box if you want to enable Parental Control for the account. Uncheck the box if Parental Control for the account should be disabled.

5. Click the **Apply** button to save the changes you have made.

To enable or disable Parental Control for an account from the Parental Control window:

1. Open the application settings window.

2. In the left part of the window, in the **Advanced Settings** section, select the **Parental Control** component.

3. In the right part of the window, select the user for whom you want to enable or disable Parental Control.

4. Click the **Control** button over the list of users to enable Parental Control for the account. If you want to disable Parental Control for the account, click the **Disable** button.

To enable or disable Parental Control for the current account from the context menu of the application icon:

1. Right-click to open the context menu of the application icon (see section "Context menu" on page 43).

2. Select **Enable Parental Control** if you want to enable control for the current account. Select **Disable Parental Control** if you want to disable control for the current account.

EXPORTING AND IMPORTING PARENTAL CONTROL SETTINGS

If you have configured Parental Control for a certain account, you can save the settings to a file (*export*). Subsequently you can load the settings from that file to configure them quickly (*import*). Furthermore, you can apply the control settings defined for another account or a configuration template (predefined set of rules for different types of users depending upon their age, experience and other characteristics).

After a certain configuration is applied to an account, you can modify the values of the settings. That will not affect the values in the source file, from which these settings have been imported.

In order to save the Parental Control settings to file, perform the following actions:

1. Open the main application window and select the **Parental Control** section in the left part of the window.

2. In the right part of the window, select the user account whose control settings should be saved.

3. In the left part of the window that opens, select the **User Account Settings** section.

4. Click the **Save** button in the lower part of the window and save the configuration file.

To load the control settings from file, perform the following steps:

1. Open the main application window and select the **Parental Control** section in the left part of the window.

2. In the right part of the window, select the user account for which the control settings should be loaded.

3. In the left part of the window that opens, select the **User Account Settings** section.

4. Click the **Load** button in the lower part of the window.

5. Use the **Load Parental Control settings** window that opens to select the **Configuration file** option and specify the file location.

To apply the settings of another account, perform the following steps:

1. Open the main application window and select the **Parental Control** section in the left part of the window.

2. In the right part of the window, select the user account for which the control settings should be loaded.
3. In the left part of the window that opens, select the **User Account Settings** section.
4. Click the **Load** button in the lower part of the window.
5. Select the **Another user** option in the **Load Parental Control settings** window that opens, and specify the account whose settings should be used.

To use a configuration template, perform the following steps:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account for which the control settings should be loaded from a template.
3. In the left part of the window that opens, select the **User Account Settings** section.
4. Click the **Load** button in the lower part of the window.
5. Select the **Template** option in the **Load Parental Control settings** window that opens, and specify the template that contains the necessary settings.

DISPLAYING AN ACCOUNT IN KASPERSKY INTERNET SECURITY

You can select an alias and an image with which your account should be displayed in Kaspersky Internet Security.

To specify an alias and an image for an account:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account whose display you want to configure.
3. In the left part of the window that opens, select the **User Account Settings** section.
4. Specify the user alias in the **Alias** field.
5. Select an image for the user account.
6. Click the **Apply** button to save the changes you have made.

TIME OF COMPUTER USE

You can set up a schedule of user's access to the computer (specifying days of week and time of day) and limit total time of computer use per 24 hours.

To limit the time of computer use:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account on which a restriction should be imposed.
3. In the left part of the window that opens, select the **Computer Usage** section.
4. In the right part of the window, check the **Enable control** box.
5. Impose time limits on computer use.
6. Click the **Apply** button to save the changes you have made.

RUNNING APPLICATIONS

You can allow or block the running of specified programs and impose time limits on startup.

To restrict programs running:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account on which a restriction should be imposed.
3. In the left part of the window that opens, select the **Running applications** section.
4. In the right part of the window, check the **Enable control** box.
5. Create the lists of allowed and blocked applications, set a schedule for the use of allowed applications.
6. Click the **Apply** button to save the changes you have made.

TIME OF INTERNET USE

You can restrict the time which the user spends in the Internet. To do this, you can set up a schedule of Internet use (specifying days of week and time of day when access should be granted or denied) and limit total time of Internet use per 24 hours.

To limit the time of Internet use:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account on which a restriction should be imposed.
3. In the left part of the window that opens, select the **Internet Usage** section.
4. In the right part of the window, check the **Enable control** box.
5. Impose time limits on Internet use.
6. Click the **Apply** button to save the changes you have made.

VIEWING WEBSITES

You can impose restrictions on access to specified websites depending on their content. To do this, you can select categories of websites to be blocked, and create a list of exclusions, if required.

You can also enable the *safe search mode*, which is used by the user when handling search engines. Some search engines are designed to protect users against unsolicited content of web resources. To do this, when indexing websites, key words and phrases, resources' addresses and categories are analyzed. When the safe search mode is enabled, search results do not include websites related to unwanted categories, such as porn, drug abuse, violence, and other materials not recommended for under-aged audiences.

Parental Control allows enabling of the safe search mode simultaneously for the following search engines:

- Google;
- Bing.com.

To restrict access to websites:

1. Open the main application window and select the **Parental Control** section in the left part of the window.

2. In the right part of the window, select the user account on which a restriction should be imposed.
3. Select the **Web Browsing** section in the left part of the displayed window.
4. In the right part of the window, check the **Enable control** box.
5. Select the categories of websites that you want to be blocked for access.
6. If you want to allow access to some websites which are blocked, or block access to some websites which are not blocked, add them into the list of exclusions. To do this, open the **Block websites: exclusions** window by clicking the **Exclusions** button.
7. Check the **Enable safe search mode** box to enable safe search mode.
8. Click the **Apply** button to save the changes you have made.

DOWNLOADING FILES FROM THE INTERNET

You can specify the types of files that the user can download from the Internet.

To restrict download of files from the Internet:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account on which a restriction should be imposed.
3. In the left part of the window that opens, select the **Downloading files** section.
4. In the right part of the window, check the **Enable control** box.
5. Select the file categories that should be allowed to download.
6. Click the **Apply** button to save the changes you have made.

COMMUNICATING VIA IM CLIENTS

Controlling communication via instant messaging programs (IM clients) consists in controlling contacts allowed for communication, blocking banned contacts, and monitoring messaging logs. You can create the lists of trusted and blocked contacts, specify key words that should be checked for in messages, and specify personal information that should not be sent out anyway.

If communication with a contact is blocked, all messages addressed to this contact or received from it will be filtered out. Information about blocked messages and key words encountered in them is displayed in a report. The report also includes messaging logs for each contact.

The following restrictions are imposed on communication monitoring:

- If an IM client had been run before Parental Control has been enabled, communication monitoring will not start until the IM client is restarted.
- When using an HTTP proxy, communication is not monitored.

The current version of Parental Control monitors communication via the following IM clients:

- ICQ;
- QIP;
- Windows Live Messenger (MSN);

- Yahoo Messenger;
- GoogleTalk;
- mIRC;
- Mail.Ru Agent;
- Psi;
- Miranda;
- AIM;
- Digsby;
- Pidgin;
- Qnext;
- SIM;
- Trilian;
- Xchat;
- Instantbird;
- RnQ;
- MSN;
- Jabber.

Some IM clients, such as Yahoo! Messenger and Google Talk use a secure connection. To scan the traffic generated by those programs, you have to enable scanning for secure connections (see page 128).

To restrict contacts available for communication via IM clients:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account on which a restriction should be imposed.
3. In the left part of the window that opens, select the **Instant Messaging** section.
4. In the right part of the window, check the **Enable control** box.
5. Create a list of allowed and blocked contacts.
6. Specify the default action for the contacts which are not included in the list: if you want to block messaging with such contacts, check the **Block messaging with other contacts** box. Uncheck this box to allow communication with contacts that have not been included into the list.
7. Click the **Apply** button to save the changes you have made.

COMMUNICATING VIA SOCIAL NETWORKS

Controlling communication via social networks consists of controlling contacts allowed for communication, blocking banned contacts, and monitoring messaging logs. You can create the lists of trusted and blocked contacts, specify key words that should be checked for in messages, and specify personal information that should not be sent out anyway.

If communication with a contact is blocked, all messages addressed to this contact or received from it will be filtered out. Information about blocked messages and key words encountered in them is displayed in a report. The report also includes messaging logs for each contact.

Some social networks, such as Twitter, use the encrypted connections. To scan the traffic generated by those networks, you should enable the scan of encrypted connections (see page 128).

To restrict contacts available for communication via social networks:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account on which a restriction should be imposed.
3. In the left part of the window that opens, select the **Social networks** section.
4. In the right part of the window, check the **Enable control** box.
5. Specify the default action for contacts that have not been included into the list of controlled ones: if you want to block communication with such contacts, check the **Block messaging with other contacts** box. Uncheck this box to allow communication with contacts that have not been included into the list of controlled ones.
6. Select the **Reports** tab.
7. In the left part of the window, select the **Social networks** section.

   In the right part of the window, a list of contacts will appear, displaying the contacts from which a message has been received or to which a message has been sent.
8. Specify an action (block or allow messaging) for the selected contacts.

   The contacts will be automatically added into the list of controlled ones which can be viewed on the **Settings** tab, in the **Social Networking** section.
9. Click the **Apply** button to save the changes you have made.

SENDING CONFIDENTIAL INFORMATION

You can block sending data that contain confidential information via IM clients, social networks, and when sending data to websites. To do this, you should create a list of records that contain privacy data, such as physical address and phone number.

Attempts of sending listed data are blocked; information about blocked messages is displayed in a report.

To block sending of private data:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account on which a restriction should be imposed.
3. In the left part of the window that opens, select the **Private data** section.
4. In the right part of the window, check the **Enable control** box.
5. Create a list of private data that should not be sent anyway.

6. Click the **Apply** button to save the changes you have made.

SEARCHING FOR KEY WORDS

You can check user's messages for specified words and word combinations when communicating via IM clients, social networks, and when sending data to websites.

If some listed key words are detected in the messages, this is displayed in a report.

If you have disabled control of messaging via IM clients, social networks, or control of websites being visited, key words are not searched for.

To monitor specified key words in messages and data being sent:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account on which a restriction should be imposed.
3. In the left part of the window that opens, select the **Key words** section.
4. In the right part of the window, check the **Enable control** box.
5. Create a list of key words to monitor in messages and data being sent.
6. Click the **Apply** button to save the changes you have made.

VIEWING REPORTS OF USER'S ACTIVITY

You can access the reports on the activity of every user account under Parental Control reviewing individually every category of the controlled events.

To view a report on the activity of a controlled user account, perform the following steps:

1. Open the main application window and select the **Parental Control** section in the left part of the window.
2. In the right part of the window, select the user account for which you want to view the report.
3. Select the **Reports** tab.
4. Use the left part of the window that opens to select the category of supervised operations or content, for example, **Internet Usage** or **Private Data**.

   A report of actions and content being supervised will be displayed in the right part of the window.

TRUSTED ZONE

Trusted zone is the user-created list of objects which should not be controlled by the application. In other words, it is a set of exclusions from the scope of Kaspersky Internet Security protection.

Trusted zone is created based on the list of trusted applications (see section "Creating a list of trusted applications" on page 166) and exclusion rules (see section "Creating the exclusion rules" on page 167), with regard for the features of the objects being processed and the applications installed on the computer. Including objects into the trusted zone may be required if, for example, Kaspersky Internet Security blocks access to an object or application although you are assured that this object / application is absolutely harmless.

For example, if you think objects being used by Microsoft Windows Notepad to be harmless and require no scan, thus trusting this application, add Notepad into the list of trusted applications to exclude scan of objects being used by this process.

Some actions classified as dangerous may be stated as safe by a number of applications. Thus, applications that automatically toggle keyboard layouts, such as Punto Switcher, regularly intercept text being entered on your keyboard. To take into account the specifics of such applications and disable the monitoring of their activity, you are advised to add them to the list of trusted applications.

When an application is added into the list of trusted ones, its file and network activities (including suspicious ones) become uncontrolled. So do its attempts to access the system registry. At the same time, the executable file and the trusted application's process is scanned for viruses as they were before. To completely exclude an application from the scan, you should use exclusion rules.

Excluding trusted applications from the scan allows to avoid problems of the application's compatibility with other programs (e.g. the problems of double scanning of network traffic of a third-party computer by Kaspersky Internet Security and by another anti-virus application), as well as increase the computer's performance rate which is critical when using server applications.

In its turn, exclusion rules of trusted zone ensure the option to work with legal applications the may be used by intruders to do harm to the user's computer or data. These applications have no malicious features, but they may be used as auxiliary components of a malicious program. This category includes remote administration applications, IRC clients, FTP servers, various utility tools for halting or concealing processes, keyloggers, password hacking programs, dialers, and others. Such applications may be blocked by Kaspersky Internet Security. To avoid blockage, you can configure exclusion rules.

Exclusion rule – is a set of conditions which determine that an object should not be scanned by Kaspersky Internet Security. In any other case, the object is scanned by all protection components according to their respective protection settings.

Exclusion rules of the trusted zone may be used by several application components, such as File Anti-Virus, Mail Anti-Virus, Web Anti-Virus (see section "Web Anti-Virus" on page 100), or when running virus scan tasks.

IN THIS SECTION:

Creating a list of trusted applications 166

Creating the exclusion rules 167

CREATING A LIST OF TRUSTED APPLICATIONS

By default, Kaspersky Internet Security scans objects being opened, run, or saved by any program process, and monitors the activity of all applications and the network traffic they create. When you add an application to the list of trusted ones, Kaspersky Internet Security excludes it from scan.

To add an application to the trusted list:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Threats and Exclusions** subsection.
3. In the **Exclusions** section, click the **Settings** button.
4. In the window that opens, on the **Trusted applications** tab, open the application selection menu by clicking the **Add** button.
5. In the menu that opens, select an application from the **Applications** list, or select **Browse** to specify the path to the executable files of the required application.
6. In the **Exclusions for applications** window that opens, check the boxes for the types of application's activity that should be excluded from scan.

You can change a trusted application or delete one from the list using the corresponding buttons in the top part of it. To remove an application from the list without its actual deletion, uncheck the box next to its name.

CREATING THE EXCLUSION RULES

If you use applications recognized by Kaspersky Internet Security as legal ones that may be used by intruders to do harm to the user's computer or data, we recommend that you configure exclusion rules for them.

To create an exclusion rule:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Threats and Exclusions** subsection.
3. In the **Exclusions** section, click the **Settings** button.
4. In the window that opens, on the **Exclusion rules** tab, click the **Add** button.
5. In the **Exclusion rule** window that opens, edit the exclusion rule settings.

PERFORMANCE AND COMPATIBILITY WITH OTHER APPLICATIONS

Performance of Kaspersky Internet Security is implied as the range of detectable threats as well as energy consumption and resource intensity.

Kaspersky Internet Security allows you to flexibly configure the protection scope and select various types of threats (see section "Selecting detectable threat categories" on page 168), that the application should detect.

Energy consumption has a great importance for portable computers. Scanning computers for viruses and updating Kaspersky Internet Security databases often require significant amounts of resources. Special laptop mode of Kaspersky Internet Security (see page 170) allows you to automatically postpone scheduled scan and update tasks when using batteries, thus saving battery charge, while Idle Scan mode (see section "Running tasks in background mode" on page 169) allows you to run resource-intensive tasks when your computer is not in use.

Consumption of the computer's resources by Kaspersky Internet Security may impact other applications' performance. To solve problems of joint operations with increased load of the CPU and disk subsystems, Kaspersky Internet Security may pause scan tasks and concede resources to other applications (see page 168) running on your computer.

In the Gaming profile mode, the application automatically disables displaying notifications of Kaspersky Internet Security's activity with other applications running in full-screen mode.

In case of an active infection in the system, the advanced disinfection procedure requires restarting your computer, which may also impact other applications' performance. If necessary, you can disable the advanced disinfection technology (see page 168) to avoid an unwanted restart of your computer.

IN THIS SECTION:

Selecting detectable threat categories 168

Advanced disinfection technology 168

Distributing computer resources when scanning for viruses 168

Running tasks in background mode 169

Application settings in full-screen mode. Gaming Profile 170

Battery saving 170

SELECTING DETECTABLE THREAT CATEGORIES

Threats detected by Kaspersky Internet Security are divided into categories by various attributes. The application always detects viruses, Trojan programs, and malicious utility tools. These programs can do significant harm to your computer. To ensure more reliable computer protection, you can extend the list of detected threats by enabling control of actions performed by legal applications that may be used by an intruder to do harm to the user's computer and data.

To select the detectable threat categories:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Threats and Exclusions** subsection.
3. In the right part of the window, click the **Settings** button located under the **Detection of the following threat types is enabled** list.
4. In the **Threats** window that opens, check the boxes for the categories of threats that should be detected.

ADVANCED DISINFECTION TECHNOLOGY

Today's malicious programs can invade the lowest levels of an operating system which makes them practically impossible to delete. If a malicious activity is detected within the system, Kaspersky Internet Security offers you to carry out a special advanced disinfection procedure which allows elimination of the threat and deletes it from the computer.

After this procedure, you will need to restart your computer. After restarting your computer, you are advised to run full virus scan (see section "How to perform full scan of your computer for viruses" on page 60).

For Kaspersky Internet Security to use the advanced disinfection procedure:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Compatibility** subsection.
3. Check the **Enable Advanced Disinfection technology** box.

DISTRIBUTING COMPUTER RESOURCES WHEN SCANNING FOR VIRUSES

Virus scan tasks may be postponed to limit the load on the central processing unit (CPU) and disk storage subsystems.

Executing scan tasks increases the load on the CPU and disk subsystems, thus slowing down other applications. By default, if such a situation arises, Kaspersky Internet Security pauses virus scan tasks and releases system resources for the user's applications.

However, there is a number of applications which start immediately when CPU resources become available, and run in the background. For the scan not to depend on the performance of those applications, system resources should not be conceded to them.

Note that this setting can be configured individually for every scan task. In this case, the configuration for a specific task has a higher priority.

For Kaspersky Internet Security to postpone scan tasks when they slow down other applications:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Compatibility** subsection.
3. Check the **Concede resources to other applications** box.

RUNNING TASKS IN BACKGROUND MODE

To optimize load on the computer resources, you can enable regular scan for rootkits in background mode and run of resource-intensive tasks when the computer is idle.

Regular scan for rootkits is run while you work at the computer. The scan takes 5 minutes at the most and involves a minimum share of the computer resources.

When the computer is idle, the following tasks can be run:

- automatic update of anti-virus databases and program modules;
- scan of system memory, startup objects, and system partition.

Idle Scan tasks are run if the computer has been blocked by the user, or if the screensaver is displayed on the screen for at least 5 minutes.

If your computer is battery-powered, no tasks are run when the computer is idle.

The first stage of Idle Scan is checking if the databases and application modules are up-to-date. If an update is required after scan, the automatic update task starts. At the second stage, the application verifies the date and status of the last run of Idle Scan. If Idle Scan has not been run at all, or has been run more than 7 days ago, or has been interrupted, then the application runs the scan task for the system memory, startup objects, and system registry.

Idle Scan is performed using deep level of heuristic analysis, which increase the probability of threat detection.

When the user returns to his or her work, the Idle Scan task is automatically interrupted. Note that the application remembers the stage at which the task has been interrupted to resume the scan from this stage later.

If running Idle Scan tasks has been interrupted while downloading an update package, the update will start from the beginning next time.

To enable regular scan for rootkits in background mode:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the **General Settings** subsection.
3. In the right part of the window, check the **Perform regular rootkit scan** box.

To enable Idle Scan mode:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the **General Settings** subsection.
3. In the right part of the window, check the **Perform idle scan** box.

APPLICATION SETTINGS IN FULL-SCREEN MODE. GAMING PROFILE

Certain programs (especially computer games) running in full-screen mode are marginally compatible with some features of Kaspersky Internet Security: for example, pop-up notifications are really undesirable in that mode. Quite often those applications require significant system resources, meaning that running certain Kaspersky Internet Security tasks may slow down their performance.

To avoid manually disabling notifications and pausing tasks every time you launch full-screen applications, Kaspersky Internet Security provides the option of temporarily changing the settings using the gaming profile. When the Gaming Profile is active, switching to full-screen mode automatically changes the settings of all product components to ensure optimal system functioning in that mode. Upon exit from the full-screen mode, product settings return to the initial values used before entering the full-screen mode.

To enable the gaming profile, perform the following tasks:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Gaming Profile** subsection.
3. Check the **Use Gaming Profile** box and specify the necessary gaming profile settings in the **Profile options** section below.

BATTERY SAVING

To save power on a portable computer, virus scan and scheduled update tasks can be postponed. If necessary, you can update Kaspersky Internet Security or start a virus scan manually.

To enable the power conservation mode and extend battery life:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Battery Saving** subsection.
3. In the right part of the window, check the box **Disable scheduled scans while running on battery power**.

KASPERSKY INTERNET SECURITY SELF-DEFENSE.

Because Kaspersky Internet Security ensures your computer protection against malware, malicious programs penetrating your computer, attempts to block Kaspersky Internet Security or even delete the application from your computer.

Stable performance of your computer's security system is ensured by features of self-defense and protection against remote access implemented in Kaspersky Internet Security.

Kaspersky Internet Security self-defense prevents modification and deletion of own files on the hard disk, processes in the memory, and entries in the system registry. Protection against remote access allows you to block all attempts to remotely control application services.

On computers running under 64-bit operating systems and Microsoft Windows Vista, Kaspersky Internet Security self-defense is only available for preventing the application's own files on local drives and system registry records from being modified or deleted.

IN THIS SECTION:

Enabling and disabling self-protection 171

Protection against external control 171

ENABLING AND DISABLING SELF-PROTECTION

By default, Kaspersky Internet Security self-defense is enabled. You can disable self-defense, if necessary.

To disable Kaspersky Internet Security Self-Defense:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Self-Defense** subsection.
3. In the right part of the window, uncheck the **Enable Self-Defense** box.

PROTECTION AGAINST EXTERNAL CONTROL

By default, protection against external control is enabled. You can disable protection, if necessary.

Frequent are situations when remote administration programs (such as RemoteAdmin) are needed while using the remote access protection. To ensure performance of these applications, you should add them to the list of trusted applications (see section "Creating a list of trusted applications" on page 166) and enable the **Do not monitor application activity** setting for them.

To disable protection against external control:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Self-Defense** subsection.
3. In the **External control** section, uncheck the **Disable external service control** box.

QUARANTINE AND BACKUP

Quarantine is a special repository that stores the objects possibly infected with viruses. *Potentially infected objects* are objects suspected of being infected with viruses or their modifications.

A potentially infected object can be detected and quarantined by File Anti-Virus, Mail Anti-Virus, Proactive Defense or in the course of a virus scan.

Objects are quarantined in the following cases:

- Object code resembles a known but partially modified threat, or has malware-like structure but is not registered in the database. In this case objects are moved to Quarantine after heuristic analysis performed by the File Anti-Virus, Mail Anti-Virus or during anti-virus scan. Heuristic analysis rarely causes false alarms.

- The sequence of operations performed by an object looks suspicious. In this case objects are moved to Quarantine after the analysis of their behavior by Proactive Defense component.

When you place an object in Quarantine, it is moved, not copied: the object is deleted from the disk or email, and saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous.

Backup storage is designed for storing backup copies of infected objects that could not been disinfected immediately after detection.

It is possible that after the next databases update, Kaspersky Internet Security will be able to identify the threat unambiguously and neutralize it. Due to this fact, the application scans quarantine objects after each update (see page 88).

IN THIS SECTION:

Storing quarantine and backup objects 172

Working with quarantined objects 172

STORING QUARANTINE AND BACKUP OBJECTS

The default maximum storage duration for objects is 30 days. Then the objects will be deleted. You can cancel the time-based restriction or change the maximum objects storage duration.

Additionally, you can specify maximum size of Quarantine and Backup. If the maximum size value is reached, the content of Quarantine and Backup is changed with new objects. By default, the maximum size restriction is disabled.

To modify the object maximum storage time:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the right part of the window, in the **Storing Quarantine and Backup objects** section check the box **Store objects no longer than** and specify maximum storage duration for quarantined objects.

To configure the maximum Quarantine and Backup size:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the right part of the window, in the **Storing Quarantine and Backup objects** section check the box **Maximum size** and specify the maximum Quarantine and Backup size.

WORKING WITH QUARANTINED OBJECTS

The quarantine of Kaspersky Internet Security lets you perform the following operations:

- quarantine the files that you suspect of being infected;
- scan and disinfect all potentially infected quarantine objects using the current database of Kaspersky Internet Security;
- restore files to a specified folder to source folders from which they were moved to quarantine (by default);
- delete any quarantined object or group of objects;

- send quarantined objects to Kaspersky Lab for analysis.

You can move an object to Quarantine using one of the two methods:

- using the **Move to Quarantine** link in the **Protection state** window;
- using the context menu of the object.

To move an object to Quarantine from the Protection state window:

1. Open the main application window.
2. Click the **Quarantine** link in the top part of the main window to open the **Protection state** window on the **Detected threats** tab.
3. Click the **Move to Quarantine** button.
4. In the window that opens, select the object that you want to move to Quarantine.

To move an object to Quarantine using the context menu:

1. Open Microsoft Windows Explorer and go to the folder that contains the object that you want to move to Quarantine.
2. Right-click to open the context menu of the object and select **Move to Quarantine**.

To scan a quarantined object:

1. Open the main application window.
2. Click the **Quarantine** link in the top part of the window and open the quarantine window.
3. In the window that opens, on the **Detected threats** tab select the object that needs to be scanned.
4. Right-click the required files to open the context menu and select **Scan**.

To disinfect all quarantined objects:

1. Open the main application window.
2. Click the **Quarantine** link in the top part of the window and open the quarantine window.
3. In the window that opens, on the **Detected threats** tab click the **Disinfect all** button.

To restore a quarantined object:

1. Open the main application window.
2. Click the **Quarantine** link in the top part of the window and open the quarantine window.
3. In the window that opens, on the **Detected threats** tab select the object that needs to be restored.
4. Right-click the required files to open the context menu and select **Restore**.

To remove quarantined objects:

1. Open the main application window.
2. Click the **Quarantine** link in the top part of the window and open the quarantine window.
3. In the window that opens, on the **Detected threats** tab select the object that needs to be removed.

4. Right-click the required object to open the context menu and select **Delete from the list**.

To send a quarantined object to Kaspersky Lab for analysis:

1. Open the main application window.
2. Click the **Quarantine** link in the top part of the window and open the quarantine window.
3. In the window that opens, on the **Detected threats** tab select the object that needs to be sent for analysis.
4. Right-click the required object to open the context menu and select **Send**.

ADDITIONAL TOOLS FOR BETTER PROTECTION OF YOUR COMPUTER

The following wizards and tools included with Kaspersky Internet Security are used to resolve specific issues concerning your computer's security:

- Rescue Disk Creation Wizard is designed to create the Rescue Disk that allows you to restore the system operability after a virus attack by booting the computer up from removable media. Rescue Disk should be used when the infection is at such a level that it is deemed impossible to disinfect the computer using anti-virus applications or malware removal utilities.
- Privacy Cleaner Wizard is designed for searching and eliminating traces of a user's activities in the system, and the operating system's settings which allow the gathering of information about user activities.
- System Restore Wizard is designed to eliminate system damage and traces of malware objects in the system.
- Browser Configuration Wizard – designed to analyze and adjust the settings of Microsoft Internet Explorer in order to eliminate its potential vulnerabilities.
- Vulnerability Scan is designed for diagnostics of vulnerabilities in the operating system and installed applications in order to detect security breaches, which may be exploited by intruders.

All the problems found by the Wizards (except the Rescue Disk Creation Wizard) are presented in groups, based on the type of danger they pose for operating system. Kaspersky Lab offers a set of actions for each group of problems which help eliminate vulnerabilities and weak points in the system's settings. Three groups of problems and, respectively, three groups of actions on them, when detected, are distinguished:

- *Strongly recommended actions* will help eliminate problems posing a serious security threat. You are advised to perform in time all the actions in this group to eliminate the threat.
- *Recommended actions* help eliminate problems posing a potential threat. You are advised to perform all actions in this group as well to provide the optimal level of protection.
- *Additional actions* help repair system damages which do not pose a current threat but may threaten your computer's security in the future. Performing these actions ensures comprehensive protection of your computer. However, in some cases, they may lead to deletion of user settings (such as cookies).

IN THIS SECTION:

Privacy Cleaner 175

Browser Configuration 176

Rolling back the changes, made by the wizards 177

PRIVACY CLEANER

When working with the computer, a user's actions are registered in the system. Saved data include the search queries entered by users and visited web sites, launched programs, opened and saved files, Microsoft Windows system event log, temporary files, etc.

All these sources of information about the user's activity may contain confidential data (including passwords) and may become available to intruders for analysis. Frequently, the user has insufficient knowledge to prevent information being stolen from these sources.

Kaspersky Internet Security includes the Privacy Cleaner Wizard. This Wizard searches for traces of user activities in the system as well as for operation system settings, which contribute to the storing of information about user activity.

Please keep in mind that the data related to user activity in the system are accumulated all the time. The launch of any file, or the opening of any document is logged. The Microsoft Windows system log registers many events occurring in the system. For this reason, repeated running of the Privacy Cleaner Wizard may detect activity traces which were not cleaned up by the previous run of the Wizard. Some files, for example the Microsoft Windows log file, may be in use by the system while the Wizard is attempting to delete them. In order to delete these files, the Wizard will suggest that you restart the system. However, during the restart, these files may be re-created and detected again as activity traces.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

To start the Privacy Cleaner Wizard:

1. Open the main application window and select the **Tools** section in the left part of the window.
2. In the right part of the window, click the **Privacy Cleaner** button.

The Wizard steps in detail.

Step 1. Starting the Wizard

Make sure the option **Perform user's activity traces diagnostics** is selected and click the **Next** button to start the Wizard.

Step 2. Activity signs search

This Wizard searches for traces of malware activities in your computer. The scan may take some time. Once the search is complete, the Wizard will proceed automatically to the next step.

Step 3. Selecting the Privacy Cleaner actions

When the search is complete, the Wizard displays the detected activity traces and actions suggested to eliminate them. The Wizard activity report is displayed as a list (see section "Additional tools for better protection of your computer" on page 174).

To view the actions within a group, click the **+** icon to the left of the group name.

To make the Wizard perform a certain action, check the box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, uncheck the box next to it.

It is strongly recommended not to uncheck the boxes selected by default because doing so will leave your computer vulnerable to threats.

Having defined the set of actions, which the Wizard will perform, click the **Next** button.

Step 4. Privacy Cleaner

The Wizard will perform the actions selected during the previous step. The elimination of activity traces may take some time. To clean up certain activity traces, computer restart may be required; the Wizard will notify you about that.

Once the clean-up is complete, the Wizard will proceed automatically to the next step.

Step 5. Wizard completion

If you wish to clean up the traces of user activity automatically whenever Kaspersky Internet Security completes work, use the last screen of the Wizard to check the box **Clean activity traces every time on Kaspersky Internet Security exit**. If you plan to remove the activity traces manually using the Wizard, do not check this box.

Click the **Finish** button to close the Wizard.

BROWSER CONFIGURATION

Microsoft Internet Explorer browser requires in certain cases special analysis and configuring since some setting values selected by the user or set by default may cause security problems.

Here are some examples of the objects and parameters used in the browser and how they are associated with potential security threats:

- **Microsoft Internet Explorer cache**. The cache stores data downloaded from the Internet, which allows not to download them next time. This allows you to reduce the amount of time spent for loading web pages and save Internet traffic. In addition to that, the cache contains confidential data, from which a history of websites visited by the user can also be obtained. Some malware objects also scan the cache while scanning the disk, and intruders can obtain, for example, the user's email addresses. You are advised to clear the cache every time you close your browser to improve the protection.

- **Display of known file types extensions**. To edit file names conveniently you can disable showing their extensions. Nevertheless, it is sometimes useful to see the file extension. File names of many malicious objects contain combinations of symbols imitating an additional file extension before the real one (e.g., example.txt.com). If the real file extension is not displayed, users can see just the file name part with the imitated extension and so they can identify a malicious object as a harmless file. To improve protection, you are advised to enable the display of files of known formats.

- **List of trusted websites**. For some websites to run correctly, you should add them to the list of trusted sites. At the same time, malicious objects can add to this list links to websites created by intruders.

Note that some settings may lead to problems with displaying certain websites (for example if they use ActiveX controls). This problem can be solved by adding these websites to the trusted zone.

Browser analysis and configuration are performed in the Browser Configuration Wizard. The wizard checks whether the latest browser updates are installed and makes sure that the current browser settings do not make the system vulnerable to malicious exploits. Once the Wizard is complete, a report is generated which can be sent to Kaspersky Lab for analysis.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

Close all Microsoft Internet Explorer windows before starting the diagnostics.

To start the Browser Configuration Wizard:

1. Open the main application window and select the **Tools** section in the left part of the window.
2. Click the **Browser Configuration** button in the right part of the window.

The Wizard steps in detail.

Step 1. Starting the Wizard

Make sure the option **Perform diagnostics for Microsoft Internet Explorer** is selected and click the **Next** button to start the Wizard.

Step 2. Microsoft Internet Explorer settings analysis

The Wizard analyzes the settings of Microsoft Internet Explorer. Searching the browser settings for problems may take some time. Once the search is complete, the Wizard will proceed automatically to the next step.

Step 3. Selecting actions to configure the browser

The problems detected at the previous step are grouped based on the degree of danger they pose to the system (see section "Additional tools for better protection of your computer" on page 174).

To view the actions within a group, click the **+** icon to the left of the group name.

To make the Wizard perform a certain action, check the box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, uncheck the box next to it.

It is strongly recommended not to uncheck the boxes selected by default because doing so will leave your computer vulnerable to threats.

Having defined the set of actions, which the Wizard will perform, click the **Next** button.

Step 4. Browser Configuration

The Wizard will perform the actions selected during the previous step. Browser configuration may take some time. Once configuring is complete, the Wizard proceeds automatically to the next step.

Step 5. Wizard completion

Click the **Finish** button to close the Wizard.

ROLLING BACK THE CHANGES, MADE BY THE WIZARDS

Some changes made at startup of the Privacy Cleaner Wizard (see section "Eliminating activity traces" on page 175), System Restore Wizard (see section "What to do if you suspect your computer of being infected" on page 65), Browser Configuration Wizard (see section "Browser configuration" on page 176), can be rolled back (cancelled).

To roll back the changes, start the respective wizard as follows:

1. Open the main application window and select the **Tools** section in the left part of the window.
2. In the right part of the window, click one of the following buttons:
   - **Privacy Cleaner** – to start Privacy Cleaner Wizard;

- **System Restore** – to start System Restore Wizard;
- **Browser Configuration** – to start Browser Configuration Wizard.

Let us take a closer look at the wizards' steps when rolling back changes.

Step 1. Starting the Wizard

Select **Roll back changes** and click the **Next** button.

Step 2. Changes search

The Wizard searches for the changes that it has made earlier and that can be rolled back. Once the search is complete, the Wizard will proceed automatically to the next step.

Step 3. Selecting changes to roll back

At this step, a report of detected changes is provided. The report is displayed as a list that includes the wizard's actions which can be rolled back.

To make the wizard roll back an action taken earlier, check the box located to the left of the action's name.

After you have created the set of actions to roll back, click the **Next** button.

Step 4. Changes rollback

The wizard rolls back the actions selected at the previous step. When the changes rollback is completed, the wizard automatically proceeds to the next step.

Step 5. Wizard completion

Click the **Finish** button to close the Wizard.

REPORTS

Events that occur during the operation of the protection components or when the Kaspersky Internet Security tasks are run, are logged in reports. You can create a detailed report for each protection component or task and configure display of data in the most convenient form. Additionally, you can filter data (see section "Data filtering" on page 179) as well as use search (see section "Events search" on page 180) through all events included in the report.

You can save report data (see section "Saving a report into a file" on page 181) in a text file, if necessary. You can also clear the reports (see section "Clearing application reports" on page 181) containing the data which are no longer useful, and adjust the settings for creating (see section "Logging non-critical events" on page 182) and storing (see section "Storing reports" on page 181) reports.

IN THIS SECTION:

Creating a report for the selected component 179

Data filtering 179

Events search 180

Saving a report to file 181

Storing reports 181

Clearing application reports 181

Logging non-critical events 182

Configuring the reminder of report availability 182

CREATING A REPORT FOR THE SELECTED COMPONENT

You can obtain a detailed report about events which occurred during the operation of each of the Kaspersky Internet Security components or during execution of its tasks.

To work with the reports conveniently, you can change the data display on the screen: group events by various parameters, select the report period, sort events by column or by importance and also hide columns.

In order to create a report on a certain component or a task, perform the following steps:

1. Open the main application window.
2. Click the **Reports** link in the top part of the window to open the reports window.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
4. In the left part of the **Detailed report** window that opens, select the component or task, for which a report should be created. When selecting the **Protection Center** item, a report is created for all protection components.

DATA FILTERING

You can filter events in the reports of Kaspersky Internet Security by one or several values in the report columns and also define complex data filtering conditions.

To filter events by the values, perform the following steps:

1. Open the main application window.
2. Click the **Reports** link in the top part of the window to open the reports window.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
4. In the right part of the **Detailed report** window that opens, move the mouse pointer to the upper left corner of the column header and click it to open the filter menu.
5. Select in the filter menu the value, which should be used to filter data.
6. Repeat the procedure for another column, if necessary.

To specify a complex filtering condition, perform the following steps:

1. Open the main application window.
2. Click the **Reports** link in the top part of the window to open the reports window.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
4. In the right part of the **Detailed report** window that opens, right-click the appropriate report column to display the context menu for it and select **Filter**.
5. In the **Custom filter** window that opens, specify the filtration conditions:
   a. Define the query limits in the right part of the window.
   b. In the left part of the window select from the **Condition** dropdown list the necessary query condition (e.g., is greater or less, equals or does not equal the value specified as the query limit).
   c. If necessary, add the second condition using logical conjunction (logical AND) or disjunction (logical OR) operations. If you wish your data query to satisfy both specified conditions, select **AND**. If only one of the two conditions is required, select **OR**.

EVENTS SEARCH

You can search a report for the necessary event using a keyword in the search line or special search window.

To find an event using the search line, perform the following steps:

1. Open the main application window.
2. Click the **Reports** link in the top part of the window to open the reports window.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
4. Enter the keyword in the search line in the right part of the **Detailed report** window that opens.

To find an event using the search window, perform the following steps:

1. Open the main application window.
2. Click the **Reports** link in the top part of the window to open the reports window.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
4. In the right part of the **Detailed report** window that opens, right-click the appropriate column header to display the context menu for it and select **Search**.
5. Specify the search criteria in the **Search** window that opens:
   a. In the **String** field, enter a key word to be searched for.
   b. In the **Column** dropdown list, select the name of the column that should be searched for the specified key word.
   c. If necessary, check the boxes for additional search settings.
6. Click the **Find next** button.

SAVING A REPORT TO FILE

The report obtained can be saved to a text file.

In order to save the report to file, perform the following actions:

1. Open the main application window.
2. Click the **Reports** link in the top part of the window to open the reports window.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
4. In the **Detailed report** window that opens create the required report and click the **Save** button.
5. In the window that opens select a folder into which you wish to save the report file, and enter the file name.

STORING REPORTS

The default maximum report storage duration is 30 days. Then the reports will be deleted. You can cancel the time-based restriction or change the maximum report storage duration.

Besides, you can also define the maximum report file size. By default, the maximum size is 1024 MB. Once the maximum size has been reached, the content of the file is replaced with new records. You can cancel any limits imposed on the report's size, or enter another value.

To modify the report maximum storage time:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the right part of the window, in the **Storing reports** section, check the **Store reports no longer than** box and specify maximum storage period for reports.

To configure the maximum report file size, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the **Storing reports** section in the right part of the window, check the box **Maximum file size** and specify maximum size for a report file.

CLEARING APPLICATION REPORTS

You can clear the reports containing data that you need no longer.

To clear reports:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the right part of the window, in the **Clear reports** section, click the **Clear** button.
4. In the **Clearing reports** window that opens, check the boxes for the reports you wish to clear.

LOGGING NON-CRITICAL EVENTS

By default, the product does not add to its reports non-critical events, registry and file system events. You can add such records to the protection reports.

To include an entry into a log of non-critical events:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the right part of the window, check the **Log non-critical events** box.

CONFIGURING THE REMINDER OF REPORT AVAILABILITY

You can create a schedule, according to which Kaspersky Internet Security reminds you about report readiness.

To create a schedule:

1. Open the main application window.
2. Click the **Reports** link in the top part of the window to open the reports window.
3. In the window that opens, on the **Report** tab, check the **Notify about the report** box and open the schedule settings window by clicking the link with the time setting.
4. In the **Report schedule** window that opens, specify the schedule settings.

APPLICATION APPEARANCE

You can change the appearance of Kaspersky Internet Security, using alternate skins. Also, the use of various active interface elements can be configured (such as the application icon in the Microsoft Windows taskbar notification area, or pop-up messages).

IN THIS SECTION:

Application skin 182

Active interface elements 183

News Agent 183

APPLICATION SKIN

All colors, fonts, icons and texts used in Kaspersky Internet Security's interface can be modified. You can create your own skins for the application, or localize application interface in another language.

To use another application skin:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Appearance** subsection.
3. Check the **Use alternative skin** box in the right part of the window section to activate a skin. Specify the folder with the skin settings in the entry field or click the **Browse** button to find this directory.

ACTIVE INTERFACE ELEMENTS

You can configure the display of active interface elements, such as notification windows or the Kaspersky Internet Security icon in the toolbar.

To configure active interface elements:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Appearance** subsection.
3. In the **Icon in the taskbar notification area** section, check or uncheck the required boxes.

NEWS AGENT

Using *News Agent*, Kaspersky Lab informs you of all important events related to Kaspersky Internet Security and protection against computer threats.

The application notifies you of the latest news by displaying a pop-up message in the taskbar notification area. In this case, the application icon changes its shape (see below). Information about the number of unread news items is also displayed in the main application window. In the context menu of the application icon, the **News** item appears; meanwhile, a news icon appears in the interface of Kaspersky Internet Security Gadget.

You can read the news in one of the following ways:

- click the icon in the taskbar notification area;
- select **News** from the context menu of the application icon;
- click the **Read news** link in the pop-up news message;
- click the **News** link in the main application window;
- click the icon which is displayed in the center of Gadget when a piece of news appears (only for Microsoft Windows Vista and Microsoft Windows 7).

The above-listed methods of opening the News Agent window are only operable if any unread news are available.

If you do not want to receive news, you can use any of the following methods to disable delivery:

- from the News Agent window (only if any unread news are available);
- from the application settings window.

To disable news delivery from the News Agent window:

1. Open the News Agent window (see instructions above).

2. Uncheck the **Always receive news** box.

To disable news delivery from the application settings window:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Appearance** subsection.
3. In the **Icon in the taskbar notification area** section, uncheck the **Enable news notifications** box.

NOTIFICATIONS

By default, if any events occur in operation, Kaspersky Internet Security notifies you of them. If you are required to select further actions, notification windows will be displayed on the screen (see section "Notification windows and pop-up messages" on page 46). When encountering any events that do not require selecting actions, the application notifies you of them with sound signals, email messages, and pop-up messages in the taskbar notification area (see section "Notification windows and pop-up messages" on page 46).

You can select methods of notification (see section "Configuring the notification method" on page 184) of events or disable notifications (see section "Enabling and disabling notifications" on page 184).

IN THIS SECTION:

Enabling and disabling notifications 184

Configuring the notification method 184

ENABLING AND DISABLING NOTIFICATIONS

By default, Kaspersky Internet Security uses various methods to notify you of all important events related to the application's operation (see section "Configuring the notification method" on page 184). You can disable the delivery of notifications.

Regardless of whether the notifications delivery is enabled or disabled, information about events that occur in the operation of Kaspersky Internet Security, is logged in the application operation report.

When you disable the notifications delivery, it does not impact the display of notification windows. To minimize the number of notification windows displayed on the screen, use the automatic protection mode (see section "Selecting protection mode" on page 76).

To disable notification delivery:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Notifications** subsection.
3. In the right part of the window, uncheck the **Enable events notifications** box.

CONFIGURING THE NOTIFICATION METHOD

The application notifies you of events using the following methods:

- pop-up messages in the taskbar notification area;
- sound notifications;

- email messages.

You can configure an individual set of notifications delivery methods for each type of events.

By default, critical notifications and notifications of application operation failures are accompanied with a sound signal. Microsoft Windows sound scheme is used as the source of sound effects. You can modify the current scheme or disable sounds.

To configure notifications delivery methods for various types of events:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Notifications** subsection.
3. In the right part of the window, check the **Enable events notifications** box and click the **Settings** button located under the box.
4. In the **Notifications** window that opens, check boxes depending on how you want to be notified of various events: by email, with a pop-up message, or with a sound signal. To avoid receiving any notifications for a specified type of events, uncheck all boxes in the line corresponding to this event.

   To allow Kaspersky Internet Security to notify you of events by email, you should adjust the email settings of notifications delivery.

To modify the email settings for notification delivering:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Notifications** subsection.
3. In the right part of the window, check the **Enable email notifications** box and click the **Settings** button.
4. In the **Email notification settings** window that opens, specify the delivery settings.

To modify the sound scheme used with notifications, perform the following steps:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Notifications** subsection.
3. In the right part of the window, check the **Use Windows Default sound scheme** box and edit the scheme in your operating system.

   If the box is unchecked, the sound scheme from previous application versions is used.

To disable sound notifications:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Notifications** subsection.
3. In the right part of the window, uncheck the **Enable sound notifications** box.

PARTICIPATING IN THE KASPERSKY SECURITY NETWORK

A great number of new threats appear worldwide on a daily basis. You can join Kaspersky Security Network to speed up the collection of statistical data on types and sources of new threats and help develop methods to neutralize them.

Kaspersky Security Network (KSN) is an infrastructure of online services that provides access to the online Knowledge Base of Kaspersky Lab which contains information about reputation of files, web resources, and software. Using data

from Kaspersky Security Network ensures an increased response time of Kaspersky Internet Security when encountering new types of threats, improves performance of some protection components, and reduces risk of false positives.

When you participate in Kaspersky Security Network, certain statistics collected while Kaspersky Internet Security protects your computer are sent to Kaspersky Lab automatically.

No personal user data is collected, processed or stored.

Participating in the Kaspersky Security Network is voluntary. You should make your decision on participation while installing Kaspersky Internet Security; however, you can change it any time later.

To enable Kaspersky Security Network:

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Feedback** subsection.
3. In the right part of the window, check the **I agree to participate in Kaspersky Security Network** box.

VALIDATING KASPERSKY INTERNET SECURITY SETTINGS

After Kaspersky Internet Security has been installed and configured, you can verify if the application is configured correctly, using a test "virus" and its modifications. A separate test is required for each protection component / protocol.

IN THIS SECTION:

Test "virus" EICAR and its modifications 187

Testing the HTTP traffic protection 188

Testing the SMTP traffic protection 189

Validating File Anti-Virus settings 189

Validating virus scan task settings 189

Validating Anti-Spam settings 190

TEST "VIRUS" EICAR AND ITS MODIFICATIONS

This test "virus" has been specially developed by EICAR (The European Institute for Computer Antivirus Research) for testing anti-virus products.

The test "virus" IS NOT a real virus, because it does not contain code that can harm your computer. However, most anti-virus products identify EICAR as a virus.

Never use real viruses to test the operation of an anti-virus product!

You can download this test "virus" from the EICAR's official website at http://www.eicar.org/anti_virus_test_file.htm.

Before downloading the file, you should pause anti-virus protection (see section "Pausing and resuming protection" on page 54) because otherwise the application would identify and process the anti_virus_test_file.htm file as an infected object transferred via HTTP.

The application identifies the file downloaded from the EICAR website as an infected object containing a virus that cannot be disinfected and performs the actions specified for this type of object.

You can also modify the standard test "virus" to verify the operation of the application. To modify the "virus", change the content of the standard test "virus" by adding one of the prefixes to it (see table below). To modify the test "virus", you can use any text or hypertext editor, such as Microsoft Notepad or UltraEdit32.

First column of the table (see below) contains the prefixes, which should be added at the beginning of the standard test "virus" to create its modifications. The second column lists all possible statuses assigned to the object, based on the results of the scan by the application. The third column indicates how the application processes objects with the specified status. Please note that the actions performed in respect of the objects are determined by the application's settings.

Once you have added a prefix to the test "virus" save the resulting file under a name reflecting the "virus" modification, for example, having added the DELE- prefix, save the file as eicar_dele.com.

Make sure you have resumed anti-virus protection after downloading the test "virus" and creating its modifications.

Table 2. Modifications of the test virus

Prefix	Object status	Object processing information
No prefix, standard test "virus".	**Infected**. Object contains code of a known virus. Disinfection impossible.	The application identifies the object as a non-disinfectable virus. An error occurs while attempting to disinfect the object; the action performed is that specified for non-disinfectable objects.
CORR-	**Corrupted**.	The application could access the object but could not scan it because it is corrupted (for example, the file structure is corrupted, or the file format is invalid). You can find the information that the object has been processed in the report on the application's operation.
WARN-	**Suspicious**. The object contains code of an unknown virus. Disinfection impossible.	The object has been considered suspicious. At the time of detection, the application databases contain no description of the procedure for disinfecting this object. You will be notified when an object of this type is detected.
SUSP-	**Suspicious**. The object contains modified code of a known virus. Disinfection impossible.	The application detected a partial correspondence of a section of object code with a section of code of a known virus. At the time of detection, the application databases contain no description of the procedure for disinfecting this object. You will be notified when an object of this type is detected.
ERRO-	**Scan error**.	An error occurred during the scan of an object. The application could not access the object, since the integrity of the object has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the object is scanned on a network resource). You can find the information that the object has been processed in the report on the application's operation.
CURE-	**Infected**. Object contains code of a known virus. Disinfectable.	Object contains a virus that can be disinfected. The application disinfects the object; the text of the virus body is replaced with the word CURE. You will be notified when an object of this type is detected.
DELE-	**Infected**. Object contains code of a known virus. Disinfection impossible.	The application identifies the object as a non-disinfectable virus. An error occurs while attempting to disinfect the object; the action performed is that specified for non-disinfectable objects. You will be notified when an object of this type is detected.

TESTING THE HTTP TRAFFIC PROTECTION

- *In order to verify that viruses are successfully detected in a data stream transferred via the HTTP protocol:*

  tryto download this test "virus" from the **EICAR**'s official website at http://www.eicar.org/anti_virus_test_file.htm.

When the computer attempts to download the test "virus", Kaspersky Internet Security detects the object, identifies it as an infected object that cannot be disinfected, and performs the action specified in the HTTP traffic scan settings for objects with this status. By default, when you attempt to download the test "virus", the connection with the website is terminated and the browser displays a message indicating that the object is infected with the EICAR-Test-File virus.

TESTING THE SMTP TRAFFIC PROTECTION

In order to detect viruses in data streams transferred using SMTP protocol, you must use an email system that uses this protocol to transfer data.

You are advised to check virus detection in different parts of outgoing mail: in message body and in attachments. Please use the EICAR test "virus" file for testing (see section "Test "virus" EICAR and its modifications" on page 187).

To test virus detection in the stream of data transferred over SMTP, perform the following steps:

1. Create a Plain text format message using an email client installed on your computer.

   A message that contains a test virus is not scanned if it is created in RTF or HTML format!

2. Depending upon the message part, in which the application should detect a virus, perform the following steps:

   - to check virus detection in message body, add the standard or modified EICAR test "virus" text to the message beginning;
   - to check virus detection in attachments, attach to the message a file containing the EICAR test "virus".

3. Send the message to the administrator.

The application detected the object, identifies it as infected, and blocks the message.

VALIDATING FILE ANTI-VIRUS SETTINGS

In order to verify that the File Anti-Virus configuration is correct:

1. Create a folder on the disk. Copy into this folder the test "virus" downloaded from the official **EICAR** website (http://www.eicar.org/anti_virus_test_file.htm) as well as all the test "virus" modifications you created.
2. Allow all events to be logged so the report file retains data on corrupted objects or objects skipped due to errors.
3. Run the test "virus" or one of its modified versions.

The File Anti-Virus intercepts the call to execute the file, scans it, and performs the action specified in the settings for objects of that status. By selecting different actions to be performed with the detected object, you can perform a full check of the component's operation.

You can view information about the results of the File Anti-Virus operation in the report about the component's operation.

VALIDATING VIRUS SCAN TASK SETTINGS

In order to verify that the virus scan task is correctly configured:

1. Create a folder on the disk. Copy the test "virus" downloaded from the official **EICAR** website (http://www.eicar.org/anti_virus_test_file.htm) into this folder together with all test "virus" modifications that you have created.
2. Create a new virus scan task and select the folder containing the set of test "viruses" as the object to scan.
3. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors.
4. Run the virus scan task.

When the scan task is running, the actions specified in the task settings are performed as suspicious or infected objects are detected. By selecting different actions to be performed with the detected object, you can perform a full check of the component's operation.

You can view all information about the virus scan task actions in the report on the component's operation.

VALIDATING ANTI-SPAM SETTINGS

You can use a test message identified as SPAM to test the anti-spam protection.

The body of the test message must contain the following line:

```
Spam is bad do not send it
```

When this message is received on the computer, Kaspersky Internet Security scans it, assigns it the "spam" status, and performs the action specified for objects of this type.

CONTACTING THE TECHNICAL SUPPORT SERVICE

If problems occur during Kaspersky Internet Security's operation, firstly check if the method for solving them is described in the documentation, help, Knowledge Base on the Kaspersky Lab Technical Support website, or on the User Forum.

If you cannot find a solution to your problem, please contact Kaspersky Lab Technical Support Service in one of the following ways:

- send a query with the help of the Personal Cabinet on the Technical Support Service website;
- by telephone.

Technical Support Service specialists will answer any of your questions about installing, activating and using the application. They will help you to eliminate the consequences of malware activities if your computer has been infected.

Before contacting the Technical Support Service, please read the Support rules for Kaspersky Lab's products (http://support.kaspersky.com/support/rules).

When you contact the Technical Support Service, service specialists may ask you to compile a report on the system status and a trace file and send them to the Technical Support Service. After Technical Support Service specialists analyze the data you have sent, they can create an AVZ script for you to help eliminate your problems.

IN THIS SECTION:

My Kaspersky Account 191

Technical support by phone 192

Creating a system state report 192

Creating a trace file 193

Sending data files 193

AVZ script execution 194

MY KASPERSKY ACCOUNT

My Kaspersky Account – your personal section on the Technical Support Service website. Using My Kaspersky Account, you can perform the following actions:

- contact Technical Support Service and Virus Lab;
- contact the Technical Support Service without using the email;
- track the status of your request in real time;
- view a detailed history of your requests to the Technical Support Service.

To log in to My Kaspersky Account, use one of the following options:

- click the **My Kaspersky Account** in the Kaspersky Internet Security main window;
- in the address bar of your browser, type https://my.kaspersky.com.

If you do not have an account yet, you can register on the My Kaspersky Account registration page https://my.kaspersky.com/registration. Enter your email address and a password to log in to My Kaspersky Account. To send a request concerning Kaspersky Internet Security usage, you will be asked to enter an activation code.

Note that some requests should not be addressed to the Technical Support Service, but instead to the Kaspersky Virus Lab. These are requests of the following types:

- unknown malicious program – you suspect that an object is malicious, while Kaspersky Internet Security does not identify it as such;
- false alarm – Kaspersky Internet Security classifies a file as a virus, yet you are sure that the file is not a virus;
- description of the malicious program – you want to get a description of a specified virus.

To send a request to the Virus Lab, you don't need to enter an activation code.

You do not need to be a registered user of My Kaspersky Account to be able to send requests to the Virus Lab from the page with the request form (http://support.kaspersky.com/virlab/helpdesk.html).

TECHNICAL SUPPORT BY PHONE

If you encounter a problem, which requires an urgent assistance, you can call your nearest Technical Support office. Before contacting Russian-speaking (http://support.kaspersky.ru/support/support_local) or international (http://support.kaspersky.com/support/international) technical support specialists, please collect the information (http://support.kaspersky.com/support/details) about your computer and the anti-virus software installed on it. This will allow our specialists to help you more quickly.

CREATING A SYSTEM STATE REPORT

When solving your problems, Kaspersky Lab Technical Support Service specialists may require a report about the system status. This report contains detailed information about running processes, loaded modules and drivers, Microsoft Internet Explorer and Microsoft Windows Explorer plug-ins, open ports, detected suspicious objects, etc.

When a system state report is created, no personal user information is collected.

To create a system state report:

1. Open the main application window (see section "Kaspersky Internet Security main window" on page 44).
2. Use the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support tools** link.
3. In the **Information for Technical Support Service** window that opens, click the **Create system state report** button.

The system state report is created in HTML and XML formats and is saved in the sysinfo.zip archive. Once the information has been gathered, you can view the report.

To view the report:

1. Open the main application window (see section "Kaspersky Internet Security main window" on page 44).

2. Use the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support tools** link.

3. In the **Information for Technical Support Service** window that opens, click the **View** button.

4. Open the sysinfo.zip archive, which contains report files.

CREATING A TRACE FILE

After installing Kaspersky Internet Security, some failures in the operating system or in the operation of individual applications may occur. The most likely cause is a conflict between Kaspersky Internet Security and the software installed on your computer, or with the drivers of your computer components. You may be asked to create a trace file for Kaspersky Lab Technical Support Service specialists to successfully resolve your problem.

To create a trace file:

1. Open the main application window (see section "Kaspersky Internet Security main window" on page 44).

2. Use the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support tools** link.

3. In the **Information for Technical Support Service** window that opens specify the trace level from the drop-down list in **Traces** section.

   It is recommended that the required trace level is clarified by a Technical Support Service specialist. In the absence of guidance from Technical Support Service, you are advised to set the trace level to **500**.

4. To start the trace process, click the **Enable** button.

5. Reconstruct the situation from when the problem occurred.

6. To stop the trace process, click the **Disable** button.

You can switch to uploading tracing results (see section "Sending data files" on page 193) to a Kaspersky Lab server.

SENDING DATA FILES

After you have created the trace files and the system state report, you need to send them to Kaspersky Lab Technical Support Service experts.

You will need a request number to upload data files to the Technical Support Service server. This number is available in your Personal Cabinet on the Technical Support Service website if your request is active.

In order to upload the data files to the Technical Support Service server:

1. Open the main application window (see section "Kaspersky Internet Security main window" on page 44).

2. Use the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support tools** link.

3. In the **Information for Technical Support Service** window that opens, in the **Actions** section, click the **Upload information for Technical Support Service to the server** button.

   The **Uploading information for Technical Support Service to the server** window will open.

4. Check the boxes next to the trace files that you want to send to the Technical Support Service and click the **Send** button.

   The **Request number** opens.

5. Specify the number assigned to your request by contacting the Technical Support Service through My Kaspersky Account, and click the **OK** button.

The selected data files are packed and sent to the Technical Support Service server.

If for any reason it is not possible to contact the Technical Support Service, the data files can be stored on your computer and later sent from the Personal Cabinet.

To save data files to disk:

1. Open the main application window (see section "Kaspersky Internet Security main window" on page 44).
2. Use the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support tools** link.
3. In the **Information for Technical Support Service** window that opens, in the **Actions** section, click the **Upload information for Technical Support Service to the server** button.

   The **Uploading information for Technical Support Service to the server** window will open.
4. Check the boxes next to the trace files that you want to send to the Technical Support Service and click the **Send** button.

   The **Request number** opens.
5. Click the **Cancel** button, and in the window that opens confirm saving the files to disk by clicking the **Yes** button.

   The archive saving window will open.
6. Specify the archive name and confirm the save.

The created archive can be sent to the Technical Support Service from the Personal Cabinet.

AVZ SCRIPT EXECUTION

Kaspersky Lab experts will analyze your problem using the trace files and the system state report. The outcome of the analysis is a sequence of actions aimed at removing the detected problems. The number of these actions can be very large.

To simplify the procedure, AVZ scripts are used. An AVZ script is a set of instructions that allow the editing of registry keys, quarantine of files, searching for classes of files and potentially quarantine files related to them, block UserMode and KernelMode interceptors, etc.

To run the scripts, the application includes an *AVZ script execution wizard*.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

You are advised not to change the text of an AVZ script received from Kaspersky Lab experts. If problems occur during script execution, please contact Technical Support Service.

To start the Wizard:

1. Open the main application window (see section "Kaspersky Internet Security main window" on page 44).
2. Use the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support tools** link.
3. In the **Information for Technical Support Service** window that opens, click the **Execute AVZ script** button.

If the script successfully executes, the Wizard closes. If an error occurs during script execution, the Wizard displays a corresponding error message.

APPENDIX

This section includes reference information which complements the document text.

IN THIS SECTION:

Subscription statuses 196

Kaspersky Internet Security notifications list 198

Working with the application from the command line 215

SUBSCRIPTION STATUSES

The following options are used to designate the subscription status:

- *Being defined*. Your request to activate the subscription has not yet been processed (some time is required for processing the request at the server). Kaspersky Internet Security works in a full-functional mode. If after a certain period of time the subscription request has not been processed, you will receive notification that the subscription status update has not been performed. In this case the application databases will not be updated any longer (for license with update subscription), and neither will computer protection be performed (for license with protection and update subscription).

- *Active*. The subscription has been activated with no fixed term, or for a certain period of time (subscription expiry date is defined).

- *Renewed*. The subscription has been renewed with no fixed term, or for a certain period of time.

- *Error*. An error occurred when updating the subscription status.

- *Expired. Grace period.* Subscription expired, or status renewal term expired. If the status renewal term has expired, update the subscription status manually. If the subscription has expired, you can renew it, by contacting the online store from which you had purchased Kaspersky Internet Security. To use a different activation code, you should first delete the key file for the subscription you are currently using.

- *Expired. Grace period expired.* Subscription expired, or grace period for license renewal expired. Please contact the subscription provider to purchase a new subscription, or to renew the existing one.

  If the subscription validity period has elapsed as well as the grace period during which license can be renewed (subscription status – *Expired*) Kaspersky Internet Security will notify you about it and will stop its attempts to renew license automatically. For license with update subscription the functionality of the application will retain except for the databases update feature. For license with protection and update subscription the application databases will not be updated, computer protection will not be performed and scan tasks will not be executed.

- *Subscription cancellation.* You canceled subscription to automatic license renewal.

- *Update is required*. Subscription status has not been updated at the proper time for whatever reason.

  If the subscription has not been renewed in time (for example, the computer was turned off when license renewal was available), you can update its status manually in the license management window (see section "Viewing license information" on page 40). Until the moment of subscription renewal, Kaspersky Internet Security ceases to update the application databases (for license with update subscription) and stops performing computer protection or executing scan tasks (for license with protection subscription).

- *Suspended*. Subscription to automatic license renewal has been suspended.

- *Resumed*. Subscription has been resumed.

In some cases, additional information about the subscription status can be displayed for a license with subscription.

KASPERSKY INTERNET SECURITY NOTIFICATIONS LIST

This section contains the list of notifications that may be displayed on the screen by Kaspersky Internet Security.

IN THIS SECTION:

Notifications in any protection mode 198

Notifications in interactive protection mode 204

NOTIFICATIONS IN ANY PROTECTION MODE

This section contains the list of notifications that may be displayed on the screen both in automatic protection mode and in interactive protection mode (see section "Selecting protection mode" on page 76). If you want to view all available notifications, switch to interactive protection mode. In this case, not only notifications described in this section will be displayed on the screen but also those displayed in interactive protection mode only (see section "Notifications in interactive protection mode" on page 204).

IN THIS SECTION:

Special treatment required 198

Hidden driver download 199

An application without digital signature is run 199

Removable drive connected 200

New network detected 200

Untrusted certificate detected 200

Request for permission to access a website from a regional domain 201

Potentially dangerous application detected 201

Quarantined file not infected 202

New product version released 202

Technical update released 203

Technical update downloaded 203

Downloaded technical update not installed 203

License expired 204

SPECIAL TREATMENT REQUIRED

When you detect a threat that is currently active in the system (for example, a malicious process in RAM or in startup objects), a notification pops up prompting you to carry out a special advanced disinfection procedure.

The notification provides the following information:

- Threat description.
- Type of threat and name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia.

  The icon is displayed next to the name of the malicious object. Click it to open the window with information about the object. Clicking the www.securelist.com/en/ link in this window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat posed by the object.
- File name of the malicious object, including the path to it.

You are asked to select one of the following actions:

- **Yes, disinfect with reboot** – perform the special disinfection procedure.

  Kaspersky Lab specialists strongly recommend that you select this option. However, note that the operating system reboots after the disinfection procedure is completed, so you are advised to save the results of current activity and close all applications before starting this procedure. When the disinfection is in progress, all applications are blocked, except for trusted ones. After restarting your computer, you are advised to run a full virus scan.
- **Do not run** – the detected object or process will be processed according to the selected action.

To apply the selected action any time such event re-occurs, check the **Apply to all objects** box.

HIDDEN DRIVER DOWNLOAD

Some malicious applications download drivers onto the computer without being noticed by the user after which the malicious application's activity cannot be controlled by Kaspersky Internet Security. Useful applications seldom use such methods for downloading drivers.

When Application Control detects an attempt to download a driver in a hidden manner, it displays a notification on the screen.

The notification provides the following information:

- Threat description.
- Name of the driver file, including the path to it.

  The icon is displayed next to the name of the file. Click it to open the window with the information about the driver.

You can select one of the following actions:

- **Allow now** – allow downloading the driver and adding it into the list of exclusions.
- **Block now** – block driver download.
- **Quarantine** – block driver download and move the driver file to Quarantine.

AN APPLICATION WITHOUT DIGITAL SIGNATURE IS RUN

When Application Control detects an application without a digital signature and with a high threat rating according to the heuristic analysis that runs on your computer, it displays a notification on the screen.

The notification provides the following information:

- Threat description.

- Name of the application being run.

  The icon is displayed next to the name of the application. Click it to open the window with information about the application.

- Information about the number of users that use the application and trust it.

You can decide if you trust the application by selecting one of the following actions:

- **Yes, I trust** – allow opening and running the application without any restrictions.
- **Restrict the application** – allow running the application although block dangerous operations.
- **Block** – block the opening and running of the application currently and in the future.

REMOVABLE DRIVE CONNECTED

When a removable drive is connected to the computer, the notification appears on the screen. You are asked to select one of the following actions:

- **Quick Scan** – scan only files stored on the removable drive that can pose a potential threat.
- **Full Scan** – scan all files stored on the removable drive.
- **Do not scan** – do not scan the removable drive.

To apply the selected action to all removable drives that may be connected in the future, check the **Always perform in such cases** box.

NEW NETWORK DETECTED

Every time your computer connects to a new zone (i.e. network), a notification pops up.

The top part of the notification provides information about the network:

- network adapter used for network connection;
- network type (for example, "wireless");
- name of the network.

The lower part of the window requests you to assign a status to the zone, and network activity is allowed on the basis of that status:

- **Yes, it is a trusted network**. It is only recommended to apply this status to zones that in your opinion are absolutely safe where your computer is not subject to attacks and attempts to gain access to your data.
- **Local network**. This status is recommended for zones with an average risk factor (for example, corporate LANs).
- **No, it is a public network**. A high-risk network in which your computer is in danger of any possible type of threat. It is recommended selecting this status for networks not protected by any anti-virus applications, firewalls, filters etc. When you select this status, the program ensures maximum security for this zone.

UNTRUSTED CERTIFICATE DETECTED

A security check for connection via the SSL protocol is performed using the installed certificate. If an invalid certificate is detected when the connection to the server is attempted (for example, if the certificate is replaced by an intruder), a notification is displayed on screen.

The notification provides the following information:

- description of the threat;
- link for viewing the certificate;
- probable causes of the error;
- URL of the web resource.

You are asked to make a decision if the network connection should be established with the untrusted certificate:

- **Yes, accept the untrusted certificate** – proceed with connecting to the web resource.
- **Deny certificate** – interrupt the connection with the website.

REQUEST FOR PERMISSION TO ACCESS A WEBSITE FROM A REGIONAL DOMAIN

A notification is displayed on the screen when attempting to access a website from a regional domain which has not been listed as allowed or blocked.

The notification provides the following information:

- description of the reason for blocking access to the website;
- name of the region to which the website belongs;
- domain, characteristics of infectiousness of websites in this domain;
- URL of the website;
- name of the application that has attempted to access the website.

You can select one of the following actions:

- **Yes, allow request** – load the website.
- **No, block request** – cancel the website from loading.

To apply the selected action to all websites from this regional domain in the future, check the **Remember for this region** box.

POTENTIALLY DANGEROUS APPLICATION DETECTED

When Activity monitor detects an application whose behavior is similar to that of malware, a notification is displayed on the screen.

The notification provides the following information:

- Threat description.
- Type and name of the potentially dangerous application.

  The icon is displayed next to the name of the application. Click it to open the window with information about the application.
- ID of the process and name of the application file, including the path to it.

- Link to the window with the application emergence log.

You can select one of the following actions:

- **Quarantine** – close the application, move the application file to Quarantine where it poses no threat to your computer's security.

  With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

  If you manually move to Quarantine a file that turns out to be not infected at the next scan, its status changes to *OK* only if the file has been scanned for three days after it had been moved to Quarantine, or later.

- **Terminate** – interrupt the application from running.

- **Allow** – allows the application to run.

- **Add to exclusions** – allow the application to perform such actions any time in the future.

QUARANTINED FILE NOT INFECTED

By default, Kaspersky Internet Security scans quarantined files after each update of the databases. If the scan of a quarantined file definitely shows that it is not infected, a notification is displayed on the screen.

The notification provides the following information:

- recommendation of restoring the quarantined file;

- name of the file, including the path to the folder in which it had been stored before it was moved to Quarantine.

You are asked to select one of the following actions:

- **Restore** – restores the file by removing it from Quarantine and moving it to the folder in which this file had been stored before it was moved to Quarantine.

- **Cancel** – leave the file in Quarantine.

NEW PRODUCT VERSION RELEASED

When a new version of Kaspersky Internet Security is released, becoming available for downloading from Kaspersky Lab servers, a notification is displayed on the screen.

The notification provides the following information:

- link to the window with detailed information about the newly released version of the application;

- size of the installation package.

You are asked to select one of the following actions:

- **Yes, download** – download the installation package of the new application version into the selected folder.

- **No** – cancel the installation package download.

If you do not want the notification of the new application version to be displayed on the screen in the future, check the **Do not inform of this update** box.

TECHNICAL UPDATE RELEASED

When a technical update of Kaspersky Internet Security is released, becoming available for downloading from Kaspersky Lab servers, a notification is displayed on the screen.

The notification provides the following information:

- number of the application version installed on your computer;
- number of the application version after the expected technical update;
- link to the window with detailed information about the technical update;
- size of the update file.

You are asked to select one of the following actions:

- **Yes, download** – download the update file into the selected folder.
- **No** – cancel the update download. This option is available if the **Do not inform of this update** box is checked (see below).
- **No, remind later** – cancel the immediate download and receive a notification of update later. This option is available if the **Do not inform of this update** box is unchecked (see below).

If you do not want this notification to be displayed on the screen in the future, check the **Do not inform of this update** box.

TECHNICAL UPDATE DOWNLOADED

When downloading the technical update of Kaspersky Internet Security from Kaspersky Lab servers is completed, a notification is displayed on the screen.

The notification provides the following information:

- number of the application version after the technical update;
- link to the update file.

You are asked to select one of the following actions:

- **Yes, install** – install the update.

  After the update is installed, you need to reboot your operating system.

- **Postpone installation** – cancel installation to perform it later.

DOWNLOADED TECHNICAL UPDATE NOT INSTALLED

If a technical update of Kaspersky Internet Security has been downloaded but not installed on your computer, a notification is displayed on the screen.

The notification provides the following information:

- number of the application version after the technical update;
- link to the update file.

You are asked to select one of the following actions:

- **Yes, install** – install the update.

  After the update is installed, you need to reboot your operating system.

- **Postpone installation** – cancel installation to perform it later.

If you do not want the notification of this update to be displayed on the screen in the future, check the **Do not ask until new version is available** box.

LICENSE EXPIRED

When the trial license expires, Kaspersky Internet Security displays a notification on the screen.

The notification provides the following information:

- length of the trial period;
- information about the application operation outcome (may include a link to more details).

You are asked to select one of the following actions:

- **Yes, purchase** – selecting this option opens the window of a browser and loads the eStore web page where you can purchase the commercial license.
- **Cancel** – reject using the application. If you select this option, the application stops performing all of its main functions (virus scan, update, real-time protection).

NOTIFICATIONS IN INTERACTIVE PROTECTION MODE

This section contains a list of notifications displayed only when the application runs in interactive protection mode (see section "Selecting protection mode" on page 76). If you do not want such notifications to be displayed on the screen, switch protection into automatic mode. In this case, notifications displayed in any protection mode (see section "Notifications in any protection mode" on page 198) will only be displayed.

IN THIS SECTION:

Network activity of an application has been detected 205

Malicious object detected 206

Vulnerability detected 207

Requesting for permission of an application's actions 207

Dangerous activity detected in the system 208

Rolling back the changes made by a dangerous application 208

Malicious application detected 209

Malicious application or legal application that may be used by intruders detected 209

Suspicious / malicious link detected 210

Dangerous object detected in traffic 210

Attempt to access a phishing website detected 211

Attempt to access the system registry detected 211

Object cannot be disinfected 212

Hidden process detected 212

Geo Filter has blocked the attempt to access the website 213

Safe Surf has blocked the website loading 213

Safe Surf has paused the website loading 214

You are advised to switch to Safe Run for Websites 214

You are advised to quit Safe Run for Websites 214

NETWORK ACTIVITY OF AN APPLICATION HAS BEEN DETECTED

If network activity of an application is detected (default option for the applications included in the **Low Restricted** or **High Restricted** groups), a notification is displayed on screen.

The notification is displayed if Kaspersky Internet Security runs in interactive mode (see section "Selecting protection mode" on page 76), and if no packet rule has been created for the application whose network activity had been detected (see page 123).

The notification contains the following information:

- name of the application and brief description of the connection that it initiates;
- information about the connection (connection type, local and remote port, address to which the connection is established);
- application run sequence.

You are asked to select one of the following actions:

- **Allow now**.
- **Block now**.
- **Create a rule**. If you select this option, the **Firewall** window opens in which you can create a rule that would regulate the network activity of an application (see section "Editing application rules" on page 124).

You can block or allow network activity of an application once or for a longer time period. To do this, perform one of the following actions:

- To block or allow network activity of an application once, select **Allow now** or **Block now**.
- To remember the selected action for the entire session of an application that has displayed network activity, select **Allow now** or **Block now** and check the **Apply to current application session** box.

  If the **Apply always** box is displayed in the window, check it and click the **always** link to change its name to **Apply to current application session**.
- To always remember the selected action for an application, select **Allow now** or **Block now** and check the **Apply always** box.

  If the **Apply to current application session** box is displayed in the window, check it and click the **to current application session** link to change its name to **Apply always**.

MALICIOUS OBJECT DETECTED

If File Anti-Virus, Mail Anti-Virus, or a virus scan detects malicious code, a notification pops up.

The notification provides the following information:

- Threat description.
- Type of threat and name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia.

  The icon is displayed next to the name of the malicious object. Click it to open the window with information about the object. Clicking the www.securelist.com/en/ link in this window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat posed by the object.
- File name of the malicious object, including the path to it.

You are asked to select one of the following responses to the object:

- **Disinfect** – attempt to disinfect the malicious object. This option is offered if the threat is already known, and the application can attempt to disinfect the object.

  Before treatment, a backup copy is made of the object in case the necessity arise to restore it or to clarify how it was infected.
- **Quarantine** – move the object to Quarantine where it will pose no threat to your computer. This option is offered if the threat is unknown, and none of the existing disinfection methods can be applied to the object.

  With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

  If you manually move to Quarantine a file that turns out to be not infected at the next scan, its status changes to *OK* only if the file has been scanned for three days after it had been moved to Quarantine, or later.

- **Delete** – delete the object. Before deletion, a backup copy of the object is created so that it could be restored later or the way of infection could be traced.

- **Skip / Block** – block access to the object, but perform no actions in respect of it; simply record information about it in a report.

  You can return to the processing of skipped objects in the report window. However, you cannot postpone the processing of objects detected in email messages.

To apply the selected action to all objects with the same status that have been detected during the current session of a protection component or task, check the **Apply to all objects** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

VULNERABILITY DETECTED

If a vulnerability is detected when running a virus scan task, a notification is displayed on the screen.

It contains the following information:

- Descriptions of the vulnerability.

- The name of the vulnerability as listed in the Kaspersky Lab Virus Encyclopedia.

  The icon is displayed next to the name. Click it to open the window with information about the vulnerability. Clicking the www.securelist.com/en/ in the window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the vulnerability.

- File name of the vulnerable object, including the path to it.

You are asked to select one of the following responses to the object:

- **Yes, fix** – eliminate the vulnerability.

- **Ignore** – take no actions on the vulnerable object.

REQUESTING FOR PERMISSION OF AN APPLICATION'S ACTIONS

If an application attempts to perform an action about whose security or necessity Kaspersky Internet Security is unaware, a notification is displayed on the screen.

The notification provides the following information:

- Name and icon of the application. Click it to open the window with information about the application.

- Description of the application's actions.

- Location of the application file.

- Application run sequence.

You can block or allow the application run by selecting one of the following actions:

- **Make trusted** – add the application to the trusted group and always allow its run.

- **Allow now** – allow the application run once.

- **Block now** – block the application run once.

- **Terminate application and make untrusted** – add the application to the untrusted group and always block it from running.

DANGEROUS ACTIVITY DETECTED IN THE SYSTEM

When Proactive Defense detects dangerous application activity on your system, a notification pops up.

The notification contains the following information:

- Threat description.
- Type of threat and name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia.

  The icon is displayed next to the name of the malicious object. Click it to open the window with information about the object. Clicking the www.securelist.com/en/ link in this window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat posed by the object.
- ID of the process and name of the application file, including the path to it.

You can select one of the following actions:

- **Quarantine** – close the application, move the application file to Quarantine where it poses no threat to your computer's security.

  With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

  If you manually move to Quarantine a file that turns out to be not infected at the next scan, its status changes to *OK* only if the file has been scanned for three days after it had been moved to Quarantine, or later.
- **Terminate** – interrupt the application from running.
- **Allow** – allows the application to run.

To apply the selected action to all objects with the same status detected in the current session of Proactive Defense operation, check the **Always perform in such cases** box. The current session is the time since the moment the component was started until the moment it was closed or the application was restarted.

If you are sure that the program detected is not dangerous, we recommend adding it to the trusted zone to avoid Kaspersky Internet Security making repeat false positives when detecting it.

ROLLING BACK THE CHANGES MADE BY A DANGEROUS APPLICATION

When running of a potentially dangerous application finishes, you are advised to roll back (cancel) the changes that it has made in the system. In this case, a notification with a request for changes rollback is displayed on the screen.

The notification provides the following information:

- Request for rollback of the changes made by a potentially dangerous application.
- Type and name of the application.

  The icon is displayed next to the name of the application. Click it to open the window with information about the application.
- ID of the process and name of the application file, including the path to it.

You can select one of the following actions:

- **Yes, roll back** – attempt to roll back the changes made by the application.
- **Skip** – cancel changes rollback.

MALICIOUS APPLICATION DETECTED

When System Watcher detects an application whose behavior completely matches the activities of malicious applications, a notification is displayed on the screen.

The notification provides the following information:

- Threat description.
- Type and name of the malicious application.

  The icon is displayed next to the name of the application. Click it to open the window with information about the application.
- ID of the process and name of the application file, including the path to it.
- Link to the window with the application emergence log.

You can select one of the following actions:

- **Quarantine** – close the application, move the application file to Quarantine where it poses no threat to your computer's security.

  With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

  If you manually move to Quarantine a file that turns out to be not infected at the next scan, its status changes to *OK* only if the file has been scanned for three days after it had been moved to Quarantine, or later.
- **Terminate** – interrupt the application from running.
- **Allow** – allows the application to run.
- **Add to exclusions** – allow the application to perform such actions any time in the future.

MALICIOUS APPLICATION OR LEGAL APPLICATION THAT MAY BE USED BY INTRUDERS DETECTED

If File Anti-Virus, Mail Anti-Virus, or the virus scan task detects a suspicious application or a legal one that can be used by intruders, a notification is displayed on the screen.

The notification provides the following information:

- Threat description.
- Type of the threat and name of the object as listed in the Kaspersky Lab Virus Encyclopedia.

  The icon is displayed next to the name of the object. Click it to open the window with information about the object. Clicking the www.securelist.com/en/ link in the window allows you to go to the Virus Encyclopedia website and obtain more details.
- Name of the object file, including the path to it.

You are asked to select one of the following responses to the object:

- **Quarantine** – move the object to Quarantine where it will pose no threat to your computer. This option is offered if the threat is unknown, and none of the existing disinfection methods can be applied to the object.

  With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

  If you manually move to Quarantine a file that turns out to be not infected at the next scan, its status changes to *OK* only if the file has been scanned for three days after it had been moved to Quarantine, or later.

- **Delete** – delete the object. Before deletion, a backup copy of the object is created so that it could be restored later or the way of infection could be traced.

- **Delete archive** - delete password-protected archive.

- **Skip / Block** – block access to the object, but perform no actions in respect of it; simply record information about it in a report.

  You can return to the processing of skipped objects in the report window. However, you cannot postpone the processing of objects detected in email messages.

- **Add to exclusions** - create an exclusion rule for this threat type.

To apply the selected action to all objects with the same status that have been detected during the current session of a protection component or task, check the **Apply to all objects** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

If you are sure that the object detected it is not malicious, we recommend adding it to the trusted zone to avoid the program from making repeat false positives when you use the object.

SUSPICIOUS / MALICIOUS LINK DETECTED

When Kaspersky Internet Security detects an attempt to go to a website with suspicious or malicious content, a special notification is displayed on the screen.

The notification provides the following information:

- description of the threat;
- name of the application (browser) using which the website is loaded;
- URL of the website or web page with a suspicious or malicious content.

You can select one of the following actions:

- **Allow** – continues the website download.
- **Block** – blocks the website download.

To apply the selected action to all websites with the same status detected in the current session of the protection component, check the **Apply to all objects** box. The current session is the time since the moment the component was started until the moment it was closed or the application was restarted.

DANGEROUS OBJECT DETECTED IN TRAFFIC

When Web Anti-Virus detects a malicious object in traffic, a special notification pops up on screen.

The notification contains the following information:

- Description of the threat or the actions performed by the application.
- Name of the application which performs the action.
- Type of threat and name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia.

  The icon is displayed next to the name of the malicious object. Click it to open the window with information about the object. Clicking the www.securelist.com/en/ link in this window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat posed by the object.
- Object location (URL).

You are asked to select one of the following responses to the object:

- **Allow** – continue the object download.
- **Block** – block the object download from the web resource.

To apply the selected action to all objects with the same status detected during the current session of a protection component or task, check the **Apply to all objects** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

ATTEMPT TO ACCESS A PHISHING WEBSITE DETECTED

When Kaspersky Internet Security detects an attempt to access a website that belongs or may belong to the phishing ones, a special notification is displayed on the screen.

The notification provides the following information:

- description of the threat;
- URL of the website.

You are asked to select one of the following actions:

- **Allow** – continues the website download.
- **Block** – blocks the website download.

To apply the selected action to all websites with the same status detected in the current session of Kaspersky Internet Security, check the **Apply to all objects** box. The current session is the time since the moment the component was started until the moment it was closed or the application was restarted.

ATTEMPT TO ACCESS THE SYSTEM REGISTRY DETECTED

When Proactive Defense detects an attempt to access system registry keys, a notification pops up.

The notification provides the following information:

- the registry key being accessed;
- name of the file of the process that initiated the attempt to access the registry keys, including the path to it.

You are asked to select one of the following actions:

- **Allow** – allows the execution of the dangerous action once;
- **Block** – blocks the dangerous action once.

To perform the action you have selected automatically every time this activity is initiated on your computer, check the **Create a rule** box.

If you are sure that any activity by the application that attempted to access system registry keys is not dangerous, add the application to the trusted application list.

OBJECT CANNOT BE DISINFECTED

In some cases, a malicious object cannot be disinfected: for example, if the file is so corrupted that the application is unable to remove malicious code from it and restore its integrity. The treatment procedure cannot be applied to several types of dangerous objects, such as Trojans. In this case, a notification is displayed on the screen.

The notification provides the following information:

- Threat description.
- Type of threat and name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia.

  The icon is displayed next to the name of the malicious object. Click it to open the window with information about the object. Clicking the www.securelist.com/en/ link in this window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat posed by the object.
- File name of the malicious object, including the path to it.

You are asked to select one of the following responses to the object:

- **Delete** – delete the object. Before deletion, a backup copy of the object is created so that it could be restored later or the way of infection could be traced.
- **Skip / Block** – block access to the object, but perform no actions in respect of it; simply record information about it in a report.

  You can return to the processing of skipped objects in the report window. However, you cannot postpone the processing of objects detected in email messages.

To apply the selected action to all objects with the same status that have been detected during the current session of a protection component or task, check the **Apply to all objects** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

HIDDEN PROCESS DETECTED

If Proactive Defense detects a hidden process in the system, a notification is displayed on the screen.

The notification provides the following information:

- Threat description.
- Type and name of threat as listed in the Kaspersky Lab Virus Encyclopedia.

  The icon is displayed next to the name. Click it to open the window with information about the threat. Clicking the www.securelist.com/en/ in the window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat.
- Name of the process file, including the path to it.

You are asked to select one of the following actions:

- **Quarantine** – close the process, move the process file to Quarantine where it poses no threat to your computer's security.

With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

If you manually move to Quarantine a file that turns out to be not infected at the next scan, its status changes to *OK* only if the file has been scanned for three days after it had been moved to Quarantine, or later.

- **Terminate** – interrupt the process.
- **Allow** – allows the execution of the process.

To apply the selected action to all hidden processes with the same status detected in the current session of Proactive Defense operation, check the **Always perform in such cases** box. The current session is the time since the moment the component was started until the moment it was closed or the application was restarted.

If you are sure that the process detected is not dangerous, we recommend adding it to the trusted zone to avoid Kaspersky Internet Security making repeat false positives when detecting it.

GEO FILTER HAS BLOCKED THE ATTEMPT TO ACCESS THE WEBSITE

Access to a website may be blocked by Web Anti-Virus on the ground that the website belongs to a specified regional domain. A domain is considered as blocked in the following cases:

- access to the domain has been blocked by the user when configuring Web Anti-Virus;
- the previous attempt to access a website of the same region was blocked by the user.

When Geo Filter (a module of Web Anti-Virus) detects an attempt to go to a website that belongs to a blocked region, a special notification is displayed in the browser window.

The notification provides the following information:

- description of the reason for blocking access to the website;
- name of the region to which the website belongs;
- domain, characteristics of infectiousness of websites in this domain;
- URL of the website.

You can select one of the following actions:

- **Back to the previous page** – open the previous page.
- **Open web resource** – load the website which belongs to a blocked domain.
- **Open Geo Filter settings** – open the Web Anti-Virus settings window on the **Geo Filter** tab.

SAFE SURF HAS BLOCKED THE WEBSITE LOADING

When Safe Surf (a module of Web Anti-Virus) detects an attempt to go to a dangerous website, a notification is displayed in the browser window.

The notification provides the following information:

- description of the reason for blocking access to the website;
- URL of the website.

You can select one of the following actions:

- **Back to the previous page** – open the previous page.
- **Open anyway** – load the website in spite of the danger it may pose.

SAFE SURF HAS PAUSED THE WEBSITE LOADING

When Safe Surf (a module of Web Anti-Virus) detects an attempt to go to a website whose security is doubtful, a notification is displayed in the browser window.

The notification provides the following information:

- description of the reason for pausing access to the website;
- URL of the website.

You can select one of the following actions:

- **Yes, open web resource** – load the website.
- **Open and add to the trusted addresses** – load the website and add its URL to the list of trusted ones to prevent Safe Surf from pausing the loading of this website.
- **Open in Safe Run for Websites** – load the website in the safe browser (only for Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome). When loading the website in Safe Run for Websites, malicious objects (if they are present on the web pages being loaded) do not pose any threat to your computer's security.
- **No, return to the previous page** – do not load the website, opening the previous page instead.

YOU ARE ADVISED TO SWITCH TO SAFE RUN FOR WEBSITES

When working with online banking, the user needs special protection, since leakages of confidential information may lead to financial losses. Therefore, Kaspersky Lab recommends that you use Safe Run for Websites that will ensure improved protection of your digital identity data when working with online banking.

When attempting to go to an online banking website, Web Anti-Virus displays a notification in the browser window.

The notification provides the following information:

- recommendation of switching to Safe Run for Websites;
- address of the online banking resource.

You are asked to select one of the following actions:

- **Open in Safe Run for Websites** – open the website using the safe browser (only for Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome).
- **Open web resource** – open the website in standard mode.
- **Back to the previous page** – open the previous page in standard mode.

YOU ARE ADVISED TO QUIT SAFE RUN FOR WEBSITES

When you work with an online banking website in Safe Run for Websites and then go to another website with different specifics, you are advised to quit the safe browser mode. If you continue working with such common website in Safe Run for Websites, this may weaken the protection of your digital identity data.

When working in Safe Run for Websites and attempting to go from an online banking website to another one, Web Anti-Virus displays a notification in the browser window.

The notification provides the following information:

- recommendation of quitting Safe Run for Websites;
- address of the website to which you have gone from the online banking website.

You are asked to select one of the following actions:

- **Open web resource in usual browser** – quit Safe Run for Websites and open the non-online-banking website in standard mode.
- **This is a bank's website, continue in Safe Run for Websites** – open the non-online-banking website without quitting Safe Run for Websites.
- **Back to the previous page** – open the previous page in Safe Run for Websites.

WORKING WITH THE APPLICATION FROM THE COMMAND LINE

You can work with Kaspersky Internet Security from the command line. The capability is provided to perform the following operations:

- activate the application;
- start and stop the application;
- start and stop application components;
- start and stop the tasks;
- obtain information on the current status of components and tasks as well as their statistics;
- start and stop virus scan tasks;
- scan selected objects;
- update databases and software modules, roll back updates;
- export and import security settings;
- open help files using the command line syntax in general and for individual commands.

Command prompt syntax:

```
avp.com <command> [options]
```

You should access the application from the command line from the application installation folder, or by specifying the full path to avp.com.

The list of commands used to control the application and its components is provided in the table below.

START	Starts a component or a task.
STOP	Stops a component or a task. The command can only be executed if the password assigned via the Kaspersky Internet Security interface is entered.

STATUS	Displays the current component or task status on screen.
STATISTICS	Displays statistics for the component or task on screen.
HELP	Displays the list of commands and command syntax information.
SCAN	Object scan for viruses.
UPDATE	Starts the application update.
ROLLBACK	Rolls back to the last Kaspersky Internet Security update made. The command can only be executed if the password assigned via the Kaspersky Internet Security interface is entered.
EXIT	Closes the application. The command can only be executed if the password assigned via the application interface is entered.
IMPORT	Import application protection settings. The command can only be executed if the password assigned via the Kaspersky Internet Security interface is entered.
EXPORT	Exports application protection settings.

Each command requires its own specific set of settings.

IN THIS SECTION:

Activating the application 216

Starting the application 217

Stopping the application 217

Managing application components and tasks 217

Virus scan 219

Updating the application 221

Rolling back the last update 222

Exporting protection settings 222

Importing protection settings 223

Creating a trace file 223

Viewing Help 224

Return codes of the command line 224

ACTIVATING THE APPLICATION

You can activate Kaspersky Internet Security using a key file.

Command syntax:

```
avp.com ADDKEY <filename>
```

The table below describes the settings of command performance.

<filename>	Application key file name with a *.key extension

Example:

```
avp.com ADDKEY 1AA111A1.key
```

STARTING THE APPLICATION

Command syntax:

```
avp.com
```

STOPPING THE APPLICATION

Command syntax:

```
avp.com EXIT /password=<your_password>
```

Parameters description is provided in table below.

<your_password>	Application password specified in the interface

Note that this command is not accepted without a password.

MANAGING APPLICATION COMPONENTS AND TASKS

Command syntax:

```
avp.com <command> <profile|task_name> [/R[A]:<report_file>]
avp.com STOP <profile|task_name> /password=<your_password> [/R[A]:<report_file>]
```

Descriptions of commands and settings are given in the table below.

<command>	You can manage Kaspersky Internet Security components and tasks from the command prompt with the following commands: START – start a protection component or a task. STOP – stop a protection component or a task. STATUS – display the current status of a protection component or a task. STATISTICS – output statistics to the screen for a protection component or a task. Note that the STOP command will not be accepted without a password.
<profile|task_name>	You can specify any protection component of Kaspersky Internet Security, component module, on-demand scan or update task as the value for the **<profile>** setting (the standard values used by the application are shown in the table below). You can specify the name of any on-demand scan or update task as the value for the **<task_name>** setting.

<your_password>	Application password specified in the interface.
/R[A]:<report_file>	**/R:<report_file>** – log only important events in the report. **/RA:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on screen, and all events are shown.

In the **<profile>** setting, you should specify one of the values given in the table below.

RTP	All protection components. The **avp.com START RTP** command runs all the protection components if the protection has been completely disabled. If the component has been disabled using the **STOP** command from the command prompt, it is not launched by the **avp.com START RTP** command. In order to start it, you should execute the **avp.com START <profile>** command, with the name of the specific protection component entered for **<profile>**. For example, **avp.com START FM**.
FW	Firewall.
HIPS	Application Control.
pdm	Proactive Defense.
FM	File Anti-Virus.
EM	Mail Anti-Virus.
WM	Web Anti-Virus. Values for Web Anti-Virus subcomponents: **httpscan (HTTP)** – scan HTTP traffic; **sc** – scan scripts.
IM	IM Anti-Virus.
AB	Anti-Banner.
AS	Anti-Spam.
PC	Parental Control.
AP	Anti-Phishing.
ids	Network Attack Blocker.
Updater	Update.
Rollback	Rolling back the last update.
Scan_My_Computer	Scan.
Scan_Objects	Custom Scan.
Scan_Quarantine	Quarantine scan.

Scan_Startup (STARTUP)	Startup Objects Scan.
Scan_Vulnerabilities (SECURITY)	Vulnerability Scan.

Components and tasks started from the command prompt are run with the settings configured in the application interface.

Examples:

- *To enable File Anti-Virus, enter the following command:*

```
avp.com START FM
```

- *To stop computer scan, enter the following command:*

```
avp.com STOP Scan_My_Computer /password=<your_password>
```

VIRUS SCAN

Starting a scan of a certain area for viruses and processing malicious objects from the command prompt generally looks as follows:

```
avp.com SCAN [<object scanned>] [<action>] [<file types>] [<exclusions>]
[<configuration file>] [<report settings>] [<advanced settings>]
```

To scan objects, you can also use the tasks created in the application by starting the one you need from the command line. The task will be run with the settings specified in the Kaspersky Internet Security interface.

Parameters description is provided in table below.

<object to scan> – this parameter gives the list of objects that are scanned for malicious code. The parameter may include several space-separated values from the list provided.	
<files>	List of paths to the files and folders to be scanned. You can enter an absolute or relative path to the file. Items on the list are separated by a space. Comments: • If the object name contains a space, it must be placed in quotation marks. • If reference is made to a specific folder, all files in this folder are scanned.
/MEMORY	RAM objects.
/STARTUP	Startup objects.
/MAIL	Mailboxes.
/REMDRIVES	All removable media drives.
/FIXDRIVES	All internal drives.
/NETDRIVES	All network drives.
/QUARANTINE	Quarantined objects.

/ALL	Full computer scan.
/@:<filelist.lst>	Path to a file containing a list of objects and catalogs to be scanned. You can enter an absolute or relative path to the file with the list. The path must be placed without quotation marks even if it contains a space. File with the list of objects should be in a text format. Each scan object should be listed on a separate line. You are advised to specify absolute paths to scan objects in the file. When specifying a relative path, you specify the path relative to the executable file of an application, not relative to the file with the list of scan objects.
<action> – this parameter determines what action will be taken with malicious objects detected during the scan. If this parameter has not been defined, the default action is the one with the value for **/i8.** If you are working in automatic mode, then Kaspersky Internet Security automatically applies the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. An action which corresponds to the **<action>** parameter value is ignored.	
/i0	Take no action in respect of the object; record information about it in the report.
/i1	Treat infected objects and if disinfection is impossible, skip.
/i2	Treat infected objects, and if disinfection fails, delete. Do not delete infected objects from compound objects. Delete infected compound objects with executable headers (sfx archives) (this is the default setting).
/i3	Treat infected objects and if disinfection fails, delete. Delete all compound objects completely if infected parts cannot be deleted.
/i4	Delete infected objects. Delete all compound objects completely if the infected parts cannot be deleted.
/i8	Prompt the user for action if an infected object is detected.
/i9	Prompt the user for action at the end of the scan.
<file types> – this parameter defines the file types that are subject to an anti-virus scan. By default, if this parameter is not defined, only infected files by contents are scanned.	
/fe	Scan only infectable files by extension.
/fi	Scan only infectable files by contents.
/fa	Scan all files.
<exclusions> – this parameter defines objects that are excluded from the scan. The parameter may include several space-separated values from the list provided.	
-e:a	Do not scan archives.
-e:b	Do not scan email databases.
-e:m	Do not scan plain text emails.
-e:<filemask>	Do not scan objects, which match the mask.
-e:<seconds>	Skip objects that are scanned for longer than the time specified in the **<seconds>** parameter.
-es:<size>	Skip objects with size (in MB) exceeding the value specified in the **<size>** setting. This setting is only available for compound files (such as archives).

<configuration file> – defines the path to the configuration file that contains the application settings for the scan. The configuration file is in text format and contains the set of command line parameters for the anti-virus scan. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.	
/C:<file_name>	Use the settings' values specified in the **<file_name>** configuration file.
<report settings> – this parameter determines the format of the report on scan results. You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on screen, and all events are shown.	
/R:<report_file>	Log important events in this file only.
/RA:<report_file>	Log all events in this file.
<advanced settings> – settings that define the use of anti-virus scanning technologies.	
/iChecker=<on|off>	Enable / disable the use of iChecker technology.
/iSwift=<on|off>	Enable / disable the use of iSwift technology.

Examples:

- *Start a scan of memory, Startup programs, mailboxes, the directories My Documents and Program Files and the file test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Scan the objects listed in the file object2scan.txt, using the configuration file scan_setting.txt for the job. Use the scan_settings.txt configuration file. When the scan is complete, create a report to log all events:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

A sample configuration file:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

UPDATING THE APPLICATION

The syntax for updating the modules of Kaspersky Internet Security and application databases from the command line is as follows:

```
avp.com UPDATE [<update_source>] [/R[A]:<report_file>] [/C:<file_name>]
```

Parameters description is provided in table below.

<update_source>	HTTP or FTP server or network folder for downloading updates. The value for the parameter may be in the form of a full path to an update source or a URL. If a path is not selected, the update source will be taken from the application update settings.
/R[A]:<report_file>	**/R:<report_file>** – log only important events in the report. **/RA:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on the screen, and all events are shown.

/C:<file_name>	Path to the configuration file that contains the Kaspersky Internet Security update settings. A configuration file is a file in plain text format containing a list of command-line parameters for an application update. You can enter an absolute or relative path to the file. If this parameter is not defined, the values for the settings in the application interface are used.

Examples:

- *Update application databases and record all events in a report:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Update the Kaspersky Internet Security modules using the settings of updateapp.ini configuration file:*

```
avp.com UPDATE /C:updateapp.ini
```

A sample configuration file:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLING BACK THE LAST UPDATE

Command syntax:

```
avp.com ROLLBACK [/R[A]:<report_file>][/password=<your_password>]
```

Parameters description is provided in table below.

/R[A]:<report_file>	**/R:<report_file>** – log only important events in the report. **/RA:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on the screen, and all events are shown.
<your_password>	Application password specified in the interface.

Note that this command is not accepted without a password.

Example:

```
avp.com ROLLBACK /RA:rollback.txt /password=<your_password>
```

EXPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com EXPORT <profile> <filename>
```

The table below describes the settings of command performance.

<profile>	Component or task with the settings being exported. For the **<profile>** setting, you can use any value listed in the "Managing application components and tasks" Help section.
<filename>	Path to the file to which the Kaspersky Internet Security settings are being exported. An absolute or a relative path may be specified. The configuration file is saved in binary format (DAT), if no other format is specified, or it is not specified at all; it can be used later to export application settings onto other computers. The configuration file can also be saved as a text file. To do so, type the *.txt* extension in the file name. Note that you cannot import protection settings from a text file. This file can only be used to specify the main settings for Kaspersky Internet Security operation.

Example:

```
avp.com EXPORT RTP c:\settings.dat
```

IMPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com IMPORT <filename>[/password=<your_password>]
```

The table below describes the settings of command performance.

<filename>	Path to the file from which the Kaspersky Internet Security settings are imported. An absolute or a relative path may be specified.
<your_password>	Kaspersky Internet Security password specified in the application interface. Security parameters can only be imported from a binary file.

Note that this command is not accepted without a password.

Example:

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

CREATING A TRACE FILE

Trace file creation may be required in case of problems in Kaspersky Internet Security operation. This will help Technical Support Service specialists to diagnose problems more accurately.

We only recommend creating trace files for troubleshooting a specific problem. Regularly enabling traces may slow down your computer and fill up your hard drive.

Command syntax:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

Parameters description is provided in table below.

[on|off]	Enable / disable trace file creation.
[file]	Output trace to file.
<trace_level>	This value can be a value from 0 (minimum level, only critical messages) to 700 (maximum level, all messages). Technical Support will tell you what trace level you need when you contact Technical Support. If the level is not specified, we recommend setting the value to 500.

Examples:

- *To disable trace file creation:*

```
avp.com TRACE file off
```

- *To create a trace file to be sent to Technical Support with a maximum trace level of 500:*

```
avp.com TRACE file on 500
```

VIEWING HELP

The following command is used to view help about the command line syntax:

```
avp.com [ /? | HELP ]
```

You can use one of the following commands to view help information about the syntax of a specific command:

```
avp.com <command> /?
avp.com HELP <command>
```

RETURN CODES OF THE COMMAND LINE

This section describes the return codes of the command line (see table below). The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a certain type of task.

GENERAL RETURN CODES	
0	Operation completed successfully
1	Invalid setting value
2	Unknown error
3	Task completion error
4	Task cancelled
VIRUS SCAN TASK RETURN CODES	
101	All dangerous objects processed
102	Hazardous objects detected

GLOSSARY

A

Activating the application

Switching the application into full-function mode. The user needs a license to activate the application.

Active license

The license currently used for the operation of a Kaspersky Lab application. The license defines the expiration date for full functionality and the license policy for the application. The application cannot have more than one license with the active status.

Additional license

A license that has been added for the operation of Kaspersky Lab application but has not been activated. The additional license enters into effect when the active license expires.

Administration server certificate

Certificate which allows Administration server authentication when connecting the Administration console to it and when exchanging data with users' computers. Administration server certificate is created at the installation of the Administration server, and is stored in the Cert subfolder of the application installation folder.

Alternate NTFS streams

NTFS data streams (alternate data streams) designed to contain additional attributes or file information.

Each file in an NTFS file system is a set of streams. One of them contains the file content that one is be able to view after opening the file, other streams (called alternate) are designed to contain meta information and ensure, for example, NTFS compatibility with other systems, such as an older file system by Macintosh called Hierarchical File System (HFS). Streams can be created, deleted, stored apart, renamed, and even run as a process.

Alternate streams can be used by intruders to transfer data secretly, or to steal them from a computer.

Application modules

Files included in the Kaspersky Lab installation package responsible for performing its main tasks. A particular executable module corresponds to each type of the task performed by the application (real-time protection, on-demand scan, updates). By running a full scan of your computer from the main window, you initiate the execution of this task's module.

Application settings

Application settings which are common for all task types, regulating the application's operation as a whole, such as application performance settings, report settings, backup storage settings.

Archive

File "containing" one or several other objects which may also be archives.

Available updates

A set of updates for Kaspersky Lab application modules including critical updates accumulated over a certain period of time and changes to the application's architecture.

B

Base of suspicious web addresses

List of web addresses, whose content can be considered to be potentially dangerous. The list is created by Kaspersky Lab specialists. It is regularly updated and is included in the Kaspersky Lab application package.

BLACK LIST OF KEY FILES

A database containing information on blacklisted Kaspersky Lab key files. Black list file content is updated together with the product databases.

BLOCKING THE OBJECT

Denying access to an object from external applications. A blocked object cannot be read, executed, changed, or deleted.

BOOT-VIRUS

A virus that infects the boot sectors of a computer's hard drive. The virus forces the system to load it into memory during reboot and to direct control to the virus code instead of the original boot loader code.

C

COMPRESSED FILE

An archive file that contains a decompression program and instructions for the operating system for executing.

D

DANGEROUS OBJECT

Object containing a virus. You are advised not to access these objects, because it may result in an infection of your computer. Once an infected object is detected, we recommend that you disinfect it using one of Kaspersky Lab's applications, or delete it if disinfection is not possible.

DATABASE OF PHISHING WEB ADDRESSES

List of web addresses, which are defined as phishing by Kaspersky Lab specialists. The database is regularly updated and part of the Kaspersky Lab application.

DATABASE UPDATE

One of the functions performed by a Kaspersky Lab application that enables it to keep protection current. In doing so, the databases are downloaded from the Kaspersky Lab update servers onto the computer and are automatically connected to the application.

DATABASES

Databases created by Kaspersky Lab's experts and containing a detailed description of all current threats to computer security as well as methods used for their detection and disinfection. These databases are constantly updated by Kaspersky Lab as new threats appear. In order to achieve a higher quality of threat detection we recommend that you copy databases from Kaspersky Lab's update servers on a regular basis.

DELETING AN OBJECT

The method of processing objects which ends in it being physically deleted from its original location (hard drive, folder, network resource). We recommend that this method be applied to dangerous objects which, for whatever reason, cannot be disinfected.

DISINFECTING OBJECTS ON RESTART

A method of processing infected objects that are being used by other applications at the moment of disinfection. Consists of creating a copy of the infected object, disinfecting the copy created, and replacing the original, infected object with the disinfected copy after the next system restart.

DISK BOOT SECTOR

A boot sector is a particular area on a computer's hard drive, floppy, or other data storage device. It contains information on the disc's file system and a boot loader program that is responsible for starting the operating system.

There exist a number of viruses that infect boot sectors, which are thus called boot viruses. The Kaspersky Lab application allows scanning boot sectors for viruses and disinfecting them if an infection is found.

DOMAIN NAME SERVICE (DNS)

Distributed system for converting the name of a host (a computer or other network device) to an IP address. DNS functions in TCP/IP networks. Particularly, DNS can also store and process reverse requests, by determining the name of a host by its IP address (PTR record). Resolution of DNS names is usually carried out by network applications, not by users.

DUAL-HOMED GATEWAY

Computer equipped with two network adapters (each of which is connected to different networks) transferring data from one network to the other.

E

EVENT SEVERITY LEVEL

Description of the event, logged during the operation of the Kaspersky Lab application. There exist four severity levels:

- **Critical event.**
- **Functional failure.**
- **Warning.**
- **Information message.**

Events of the same type may have different severity levels, depending on the situation when the event occurred.

EXCLUSION

Exclusion is an object excluded from the scan by Kaspersky Lab application. You can exclude files of certain formats, file masks, a certain area (for example, a folder or a program), application processes, or objects by threat type, according to the Virus Encyclopedia classification from the scan. Each task can be assigned a set of exclusions.

F

FALSE ALARM

Situation when Kaspersky Lab's application considers a non-infected object as infected due to its code similar to that of a virus.

FILE MASK

Representation of a file name and extension using wildcards. The two standard wildcards used in file masks are * and ?, where * represents any number of characters and ? stands for any single character. Using these wildcards, you can represent any file. Note that the name and extension are always separated by a period.

H

HARDWARE PORT

Socket on a hardware component of a computer in which a cable or a plug can be connected (LPT port, serial port, USB port).

HEADER

The information in the beginning of a file or a message, which is comprised of low-level data on file (or message) status and processing. In particular, the email message header contains such data as information about the sender and recipient, and the date.

HEURISTIC ANALYZER

Threat detection technology for threats that cannot be detected using Anti-Virus databases. It allows detecting objects suspected of being infected with an unknown virus or a new modification of known viruses.

The use of a heuristic analyzer detects up to 92% of threats. This mechanism is fairly effective and very rarely leads to false positives.

Files detected by the heuristic analyzer are considered suspicious.

HOOK

Subcomponent of the application responsible for scanning specific types of email. The set of interceptors specific to your installation depends on what role or what combination of roles the application is being deployed for.

I

ICHECKER TECHNOLOGY

iChecker is a technology that increases the speed of anti-virus scans by excluding objects that have remained unchanged since their last scan, provided that the scan parameters (the anti-virus database and settings) have not changed. The information for each file is stored in a special database. This technology is used in both real-time protection and on-demand scan modes.

For example, you have an archive scanned by Kaspersky Lab application and assigned the not infected status. The next time the application will skip this archive, unless it has been altered or the scan settings have been changed. If you altered the archive content by adding a new object to it, modified the scan settings or updated the anti-virus database, the archive is re-scanned.

Limitations of iChecker technology:

- this technology does not work with large-size files, since it is faster to scan a file than check whether it was modified since it was last scanned;
- the technology supports a limited number of formats (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

INCOMPATIBLE APPLICATION

An antivirus application from a third-party developer or a Kaspersky Lab application that does not support management through Kaspersky Internet Security.

INFECTABLE OBJECT

An object which, due to its structure or format, can be used by intruders as a "container" to store and distribute a malicious object. As a rule, they are executable files, for example, files with the .com, .exe, .dll extensions, etc. The risk of activating malicious code in such files is fairly high.

INFECTED OBJECT

Object containing a malicious code. It is detected when a section of the object's code completely matches a section of the code of a known threat. Kaspersky Lab does not recommend using such objects since they may infect your computer.

INPUT/OUTPUT PORT

Serves in processors (such as Intel) for exchanging data with hardware components. The input/output port is associated with a certain hardware component, and allows applications to address it for data exchange.

INSTALLATION WITH A STARTUP SCENARIO

Method of remote installation of Kaspersky Lab's applications which allows assigning the startup of remote installation task to an individual user account (or to several user accounts). Registering a user in a domain leads to an attempt to install the application on the client computer on which the user has been registered. This method is recommended for installing the applications on computers running under Microsoft Windows 98 / Me operating systems.

INTERNET PROTOCOL (IP)

The basic protocol for the Internet, used without change since the time of its development in 1974. It performs basic operations in transmitting data from one computer to another and serves as the foundation for higher-level protocols like TCP and UDP. It manages connection and error processing. Technologies such as NAT and masking make it possible to hide a large number of private networks using a small number of IP addresses (or even one address), which make it possible to respond to the demands of the constantly growing Internet using the relatively restricted IPv4 address space.

K

KASPERSKY LAB'S UPDATE SERVERS

A list of Kaspersky Lab's HTTP and FTP servers from which the application downloads databases and module updates to your computer.

KASPERSKY SECURITY NETWORK

Kaspersky Security Network (KSN) is an infrastructure of online services that provides access to the online Knowledge Base of Kaspersky Lab which contains information about reputation of files, web resources, and software. Using data from Kaspersky Security Network ensures an increased response time of Kaspersky Internet Security when encountering new types of threats, improves performance of some protection components, and reduces risk of false positives.

KEY FILE

File with the .key extension, which is your personal "key", necessary for working with the Kaspersky Lab application. A key file is included with the product if you purchased it from Kaspersky Lab distributors or is emailed to you if you purchased the product online.

L

LICENSE VALIDITY PERIOD

Period of time during which you are able to use all features of your Kaspersky Lab application. The license validity period generally runs for one calendar year from the date of installation. After the license expires, the application has reduced functionality. You will not be able to update the application databases.

LIST OF ALLOWED URLS

List of masks and addresses of web resources, the accessing of which is not blocked by the Kaspersky Lab application. The list of addresses is created by the user during application settings configuration.

LIST OF ALLOWED SENDERS

(as well as "White" list of addresses)

The list of email addresses which send the messages that should not be scanned by Kaspersky Lab application.

LIST OF BLOCKED URLS

List of masks and addresses of web resources, access to which is blocked by the Kaspersky Lab application. The list of addresses is created by the user during application settings configuration.

LIST OF BLOCKED SENDERS

(also "Black" list of addresses)

The list of email addresses which send messages that should be blocked by the Kaspersky Lab application, regardless of their content.

LIST OF CHECKED WEB ADDRESSES

List of masks and addresses of web resources, which are mandatorily scanned for malicious objects by the Kaspersky Lab application.

LIST OF TRUSTED URLS

List of masks and addresses of web resources whose content the user trusts. Kaspersky Lab application does not scan web pages, corresponding to a list item, for the presence of malicious objects.

M

MAIL DATABASES

Databases containing emails in a special format and saved on your computer. Each incoming/outgoing email is placed in the mail database after it is received/sent. These databases are scanned during a full computer scan.

Incoming and outgoing emails at the time that they are sent and received are analyzed for viruses in real time if real-time protection is enabled.

MESSAGE DELETION

Method of processing an email message that contains spam signs, at which the message is physically removed. It is advised to apply this method to messages which unambiguously contain spam. Before deleting a message, a copy of it is saved in the backup (unless this option is disabled).

MONITORED OBJECT

A file transferred via HTTP, FTP, or SMTP protocols across the firewall and sent to a Kaspersky Lab application to be scanned.

MOVING OBJECTS TO QUARANTINE

A method of processing a potentially infected object by blocking access to the file and moving it from its original location to the Quarantine folder, where the object is saved in encrypted form, which rules out the threat of infection.

N

NETWORK PORT

TCP and UDP parameter that determines the destination of data packets in IP format that are transmitted to a host over a network and makes it possible for various programs running on a single host to receive data independently of each other. Each program processes data received via a certain port (this is sometimes referred to as the program "listening" to that port).

For some common network protocols, there are usually standard port numbers (for example, web servers usually receive HTTP requests on TCP port 80); however, generally, a program can use any protocol on any port. Possible values: 1 to 65535.

NOTIFICATION TEMPLATE

Template based on which a notification of infected objects detected by the scan, is generated. Notification template includes a combination of settings regulating the mode of notification, the way of spreading, and the text of messages to be sent.

O

OLE OBJECT

An attached object or an object embedded into another file. Kaspersky Lab application allows scanning OLE objects for viruses. For example, if you insert a Microsoft Office Excel table into a Microsoft Office Word document, the table is scanned as an OLE object.

OBJECT DISINFECTION

The method used for processing infected objects that results in complete or partial recovery of data, or the decision that the objects cannot be disinfected. Objects are disinfected using the database records. Part of the data may be lost during disinfection.

OBSCENE MESSAGE

Email message containing offensive language.

P

PHISHING

Kind of Internet fraud which consists in sending email messages with the purpose of stealing confidential information - as a rule, various financial data.

POTENTIALLY INFECTED OBJECT

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Potentially infected files are detected using heuristic analyzer.

PROTECTION STATUS

The current status of protection, summarizing the degree of security of the computer.

PROTOCOL

Clearly defined and standardized set of rules governing the interaction between a client and a server. Well-known protocols and the services associated with them include HTTP (WWW), FTP, and NNTP (news).

PROXY SERVER

Computer network service which allows users to make indirect requests to other network services. First, a user connects to a proxy server and requests a resource (e.g., a file) located on another server. Then, the proxy server either connects to the specified server and obtains the resource from it, or returns the resource from its own cache (in case if the proxy has its own cache). In some cases, a user's request or a server's response can be modified by the proxy server for certain purposes.

Q

QUARANTINE

A certain folder, where all possibly infected objects are placed, which were detected during scans or by real-time protection.

R

REAL-TIME PROTECTION

The application's operating mode under which objects are scanned for the presence of malicious code in real time.

The application intercepts all attempts to open any object (read, write, or execute) and scans the object for threats. Uninfected objects are passed on to the user; objects containing threats or suspected of containing them are processed pursuant to the task settings (they are disinfected, deleted or quarantined).

RECOMMENDED LEVEL

Level of security based on application settings recommended by Kaspersky Lab experts to provide the optimal level of protection for your computer. This level is set to be used by default.

RESTORATION

Moving an original object from Quarantine or Backup to the folder where it was originally found before being moved to Quarantine, disinfected, or deleted, or to a different folder specified by the user.

S

SCRIPT

A small computer program or an independent part of a program (function) which, as a rule, has been developed to execute a small specific task. It is most often used with programs embedded into hypertext. Scripts are run, for example, when you open a certain website.

If real-time protection is enabled, the application tracks the scripts launching, intercepts and scans them for viruses. Depending on the results of the scan, you may block or allow the execution of a script.

SECURITY LEVEL

The security level is defined as a pre-set component configuration.

SOCKS

Proxy server protocol that allows establishing a point-to-point connection between computers in the internal and external networks.

SPAM

Unsolicited mass email mailings, most often including advertising messages.

STARTUP OBJECTS

The set of programs needed to start and correctly operate the operating system and software installed on your computer. These objects are executed every time the operating system is started. There are viruses capable of infecting such objects specifically, which may lead to, for example, blocking your access to the operating system.

SUBNET MASK

Subnet mask (also known as netmask) and network address determine the addresses of computers on a network.

SUSPICIOUS MESSAGE

Message that cannot be unambiguously considered spam, but it seems suspicious when scanned (e.g., certain types of mailings and advertising messages).

SUSPICIOUS OBJECT

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Suspicious objects are detected using the heuristic analyzer.

T

TASK

Functions performed by Kaspersky Lab's application are implemented as tasks, such as: Real-time file protection, Full computer scan, Database update.

TASK SETTINGS

Application settings which are specific for each task type.

THREAT RATING

Rate of how dangerous an application is for the operating system. The rating is calculated using the heuristic analysis based on two types of criteria:

- static (such as information about the executable file of an application: size, creation date, etc.);
- dynamic, which are used while simulating the application's operation in a virtual environment (analysis of the application's calls to system functions).

Threat rating allows detecting a behavior typical of malware. The lower the threat rating is, the more actions the application will be allowed to perform in the system.

TRAFFIC SCAN

A real-time scan using information from the latest version of the databases for objects transmitted via all protocols (for example, HTTP, FTP, etc.).

TRUSTED PROCESS

Application process whose file operations are not monitored by Kaspersky Lab's application in real-time protection mode. In other words, no objects run, open, or saved by the trusted process are scanned.

U

UNKNOWN VIRUS

A new virus about which there is no information in the databases. Generally unknown viruses are detected by the application in objects using the heuristic analyzer, and those objects are classified as potentially infected.

UPDATE

The procedure of replacing/adding new files (databases or application modules) retrieved from the Kaspersky Lab update servers.

UPDATE PACKAGE

File package for updating the software. It is downloaded from the Internet and installed on your computer.

URGENT UPDATES

Critical updates to Kaspersky Lab application modules.

V

VIRUS ACTIVITY THRESHOLD

The maximum permissible level of a specific type of event over a limited time period that, when exceeded, is considered to be excessive virus activity and a threat of a virus outbreak. This feature is significant during virus outbreaks and enables an administrator to react in a timely fashion to threats of virus outbreaks that arise.

VIRUS OUTBREAK

A series of deliberate attempts to infect a computer with a virus.

VIRUS OUTBREAK COUNTER

Template based on which a notification of virus outbreak threat is generated. Virus outbreak counter includes a combination of settings which determine the virus activity threshold, the way of spreading, and the text in messages to be sent.

KASPERSKY LAB

Kaspersky Lab was founded in 1997. Today it is the leading developer of a wide range of high-performance information security software products, including anti-virus, anti-spam and anti-hacking systems.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has offices in the United Kingdom, France, Germany, Japan, the Benelux countries, China, Poland, Romania and the USA (California). A new company office, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network includes over 500 companies worldwide.

Today, Kaspersky Lab employs over a thousand highly qualified specialists, including 10 MBA degree holders and 16 PhD degree holders. All Kaspersky Lab's senior anti-virus experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. A thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many of the modern standards for anti-virus software. The company's flagship product, Kaspersky Anti-Virus, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

Kaspersky Lab's customers enjoy a wide range of additional services that ensure both stable operation of the company's products, and full compliance with their specific business requirements. We design, implement and support corporate anti-virus systems. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with 24-hour technical support service in several languages.

If you have any questions, comments, or suggestions, you can contact us through our dealers, or at Kaspersky Lab directly. We will be glad to assist you, by phone or email, with any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.securelist.com
Anti-Virus Lab:	newvirus@kaspersky.com (only for sending suspicious objects in archives) http://support.kaspersky.com/virlab/helpdesk.html (for sending requests to virus analysts)
Kaspersky Lab web forum:	http://forum.kaspersky.com

INFORMATION ABOUT THIRD-PARTY CODE

Third-party code was used during the application development.

IN THIS SECTION:

Program code 235

Development tools 264

Distributed program code 268

Other information 277

PROGRAM CODE

Third-party program code was used during the application development.

IN THIS SECTION:

AGG 2.4 237

ADOBE ABI-SAFE CONTAINERS 1.0 238

BOOST 1.39.0 238

BZIP2/LIBBZIP2 1.0.5 238

CONVERTUTF 238

CURL 7.19.4 239

DEELX - REGULAR EXPRESSION ENGINE 1.2 239

EXPAT 1.2, 2.0.1 239

FASTSCRIPT 1.90 240

FDLIBM 5.3 240

FLEX: THE FAST LEXICAL ANALYZER 2.5.4 240

FMT.H 240

GDTOA 240

GECKO SDK 1.8, 1.9, 1.9.1 241

ICU4C 4.0.1 249

INFO-ZIP 5.51 249

JSON4LUA 0.9.30 250

LIBGD 2.0.35 250

LIBJPEG 6B 251

LIBM (lrint.c v 1.4, lrintf.c,v 1.5) 252

LIBPNG 1.2.8, 1.2.9, 1.2.42 253

LIBUNGIF 3.0 253

LIBXDR 253

LREXLIB 2.4 254

LUA 5.1.4 254

LZMALIB 4.43 255

MD5.H 255

MD5.H 255

MD5-CC 1.02 255

OPENSSL 0.9.8K 256

PCRE 7.7, 7.9 257

SHA1.C 1.2 259

STLPORT 5.2.1 259

SVCCTL.IDL 259

TINYXML 2.5.3 259

VISUAL STUDIO CRT SOURCE CODE 8.0 259

WINDOWS TEMPLATE LIBRARY 8.0 260

ZLIB 1.0.4, 1.0.8, 1.2.2, 1.2.3 264

AGG 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

Anti-Grain Geometry has dual licensing model. The Modified BSD License was first added in version v2.4 just for convenience. It is a simple, permissive non-copyleft free software license, compatible with the GNU GPL. It's well proven and recognizable. See http://www.fsf.org/licensing/licenses/index_html#ModifiedBSD for details.

Note that the Modified BSD license DOES NOT restrict your rights if you choose the Anti-Grain Geometry Public License.

Anti-Grain Geometry Public License

Anti-Grain Geometry – Version 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

Permission to copy, use, modify, sell and distribute this software is granted provided this copyright notice appears in all copies. This software is provided "as is" without express or implied warranty, and with no claim as to its suitability for any purpose.

Modified BSD License

Anti-Grain Geometry – Version 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ADOBE ABI-SAFE CONTAINERS 1.0

Copyright (C) 2005, Adobe Systems Incorporated

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVEN SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BOOST 1.39.0

Copyright (C) 2008, Beman Dawes

BZIP2/LIBBZIP2 1.0.5

Copyright (C) 1996-2007 Julian R Seward.

CONVERTUTF

Copyright (C) 2001-2004, Unicode, Inc

Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Limitations on Rights to Redistribute This Code Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

CURL 7.19.4

Copyright (C) 1996-2009, Daniel Stenberg

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2009, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

DEELX - REGULAR EXPRESSION ENGINE 1.2

Copyright (C) 2006, RegExLab.com

http://www.regexlab.com/deelx/

EXPAT 1.2, 2.0.1

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd and Clark Cooper

Copyright (C) 2001, 2002, 2003, 2004, 2005, 2006, Expat maintainers

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FASTSCRIPT 1.90

Copyright (C) Fast Reports Inc

FDLIBM 5.3

Copyright (C) 2004, Sun Microsystems, Inc

Permission to use, copy, modify, and distribute this software is freely granted, provided that this notice is preserved.

FLEX: THE FAST LEXICAL ANALYZER 2.5.4

Copyright (C) 1990, The Regents of the University of California

---

This code is derived from software contributed to Berkeley by Vern Paxson.

The United States Government has rights in this work pursuant to contract no. DE-AC03-76SF00098 between the United States Department of Energy and the University of California.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

FMT.H

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

GDTOA

Copyright (C) 1998-2002, Lucent Technologies

Copyright (C) 2004, 2005, 2009, David M. Gay

Copyright (C) 1998-2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that the copyright notice and this permission notice and warranty disclaimer appear in supporting documentation, and that the name of Lucent or any of its entities not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

LUCENT DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL LUCENT OR ANY OF ITS ENTITIES BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 2004, 2005, 2009 David M. Gay

Permission to use, copy, modify, and distribute this software and its

documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that the copyright notice and this permission notice and warranty disclaimer appear in supporting documentation, and that the name of the author or any of his current or former employers not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR OR ANY OF HIS CURRENT OR FORMER EMPLOYERS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

GECKO SDK 1.8, 1.9, 1.9.1

Copyright (C) Mozilla Foundation

Mozilla Public License Version 1.1

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims: under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale,

have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the legal file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4 (a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3.1, 3.2, 3.3, 3.4 and 3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. Disclaimer of warranty

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

8. Termination

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

10. U.S. government end users

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48

C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. Miscellaneous

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. Responsibility for claims

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. Multiple-licensed code

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

Exhibit A - Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License

Version 1.1 (the "License"); you may not use this file except in

compliance with the License. You may obtain a copy of the License at

http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS"

basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the

License for the specific language governing rights and limitations

under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____

_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms

of the _____ license (the "[___] License"), in which case the

provisions of [_____] License are applicable instead of those

above. If you wish to allow use of your version of this file only

under the terms of the [____] License and not to allow others to use

your version of this file under the MPL, indicate your decision by

deleting the provisions above and replace them with the notice and

other provisions required by the [___] License. If you do not delete

the provisions above, a recipient may use your version of this file

under either the MPL or the [___] License."

NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.

AMENDMENTS

The Netscape Public License Version 1.1 ("NPL") consists of the Mozilla Public License Version 1.1 with the following Amendments,

including Exhibit A-Netscape Public License. Files identified with "Exhibit A-Netscape Public License" are governed by the Netscape

Public License Version 1.1.

Additional Terms applicable to the Netscape Public License.

I. Effect.

These additional terms described in this Netscape Public License -- Amendments shall apply to the Mozilla Communicator

client code and to all Covered Code under this License.

II. "Netscape's Branded Code" means Covered Code that Netscape distributes and/or permits others to distribute under one or more trademark(s) which are controlled by Netscape but which are not licensed for use under this License.

III. Netscape and logo.

This License does not grant any rights to use the trademarks "Netscape", the "Netscape N and horizon" logo or the "Netscape

lighthouse" logo, "Netcenter", "Gecko", "Java" or "JavaScript", "Smart Browsing" even if such marks are included in the Original

Code or Modifications.

IV. Inability to Comply Due to Contractual Obligation.

Prior to licensing the Original Code under this License, Netscape has licensed third party code for use in Netscape's Branded Code.

To the extent that Netscape is limited contractually from making such third party code available under this License, Netscape may

choose to reintegrate such code into Covered Code without being required to distribute such code in Source Code form, even if

such code would otherwise be considered "Modifications" under this License.

V. Use of Modifications and Covered Code by Initial Developer.

V.1. In General.

The obligations of Section 3 apply to Netscape, except to the extent specified in this Amendment, Section V.2 and V.3.

V.2. Other Products.

Netscape may include Covered Code in products other than the Netscape's Branded Code which are released by Netscape during the two (2) years following the release date of the Original Code, without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

V.3. Alternative Licensing.

Netscape may license the Source Code of Netscape's Branded Code, including Modifications incorporated therein, without such Netscape Branded Code becoming subject to the terms of this License, and may license such Netscape Branded Code on different terms from those contained in this License.

VI. Litigation.

Notwithstanding the limitations of Section 11 above, the provisions regarding litigation in Section 11(a), (b) and (c) of the License shall apply to all disputes relating to this License.

EXHIBIT A-Netscape Public License.

"The contents of this file are subject to the Netscape Public

License Version 1.1 (the "License"); you may not use this file

except in compliance with the License. You may obtain a copy of

the License at http://www.mozilla.org/NPL/

Software distributed under the License is distributed on an "AS

IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or

implied. See the License for the specific language governing

rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released

March 31, 1998.

The Initial Developer of the Original Code is Netscape

Communications Corporation. Portions created by Netscape are

Copyright (C) 1998-1999 Netscape Communications Corporation. All

Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the

terms of the _____ license (the "[___] License"), in which case

the provisions of [_____] License are applicable instead of

those above. If you wish to allow use of your version of this

file only under the terms of the [____] License and not to allow

others to use your version of this file under the NPL, indicate

your decision by deleting the provisions above and replace them

with the notice and other provisions required by the [___]

License. If you do not delete the provisions above, a recipient

may use your version of this file under either the NPL or the

[___] License."

ICU4C 4.0.1

Copyright (C) 1995-2008, International Business Machines Corporation and others

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

JSON4LUA 0.9.30

Copyright (C) 2009, Craig Mason-Jones

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBGD 2.0.35

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Cold Spring Harbor Laboratory. Funded under Grant

P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000, 2001, 2002 Philip Warner.

Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs.

Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@lucent.com).

Portions relating to gdft.c copyright 2001, 2002 John Ellson (ellson@lucent.com).

Portions copyright 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007 Pierre-Alain Joye (pierre@libgd.org).

Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information.

Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

LIBJPEG 6B

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

==========

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)

2. You can use this software for whatever you want. You don't have to pay us.

3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBM (LRINT.C V 1.4, LRINTF.C,V 1.5)

Copyright (C) 2004, Matthias Drochner

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBPNG 1.2.8, 1.2.9, 1.2.42

Copyright (C) 2004, 2006-2009, Glenn Randers-Pehrson

LIBUNGIF 3.0

Copyright (C) 1997, Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBXDR

Copyright (C) Sun Microsystems, Inc

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

LREXLIB 2.4

Copyright (C) 2000-2008, Reuben Thomas Copyright (C) 2004-2008, Shmuel Zeigerman

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LUA 5.1.4

Copyright (C) 1994-2008, Lua.org, PUC-Rio

Lua License

Lua is licensed under the terms of the MIT license reproduced below.

This means that Lua is free software and can be used for both academic and commercial purposes at absolutely no cost.

For details and rationale, see http://www.lua.org/license.html .

Copyright (C) 1994-2008 Lua.org, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LZMALIB 4.43

MD5.H

Copyright (C) 1999, Aladdin Enterprises

MD5.H

Copyright (C) 1990, RSA Data Security, Inc

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

MD5-CC 1.02

Copyright (C) 1991-1992, RSA Data Security, Inc

Copyright (C) 1995, Mordechai T. Abzug

This software contains a C++/object oriented translation and modification of MD5 (version 1.02) by Mordechai T. Abzug. Translation and modification (c) 1995 by Mordechai T. Abzug

Copyright 1991-1992 RSA Data Security, Inc.

The MD5 algorithm is defined in RFC 1321. This implementation is derived from the reference C code in RFC 1321 which is covered by the following copyright statement:

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

OPENSSL 0.9.8K

Copyright (C) 1998-2008, The OpenSSL Project

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==========

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project

for use in the OpenSSL Toolkit. (http://www.openssl.org/)" 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

PCRE 7.7, 7.9

Copyright (C) 1997-2009, University of Cambridge

Copyright (C) 2007-2008, Google Inc

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 7 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England.

Copyright (c) 1997-2009 University of Cambridge

All rights reserved.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

Copyright (c) 2007-2008, Google Inc.

All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

End

SHA1.C 1.2

Author Steve Reid (steve@edmweb.com)

STLPORT 5.2.1

Copyright (C) 1994, Hewlett-Packard Company

Copyright (C) 1996-1999, Silicon Graphics Computer Systems, Inc.

Copyright (C) 1997, Moscow Center for SPARC Technology

Copyright (C) 1999-2003, Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

SVCCTL.IDL

Copyright (C) 2010, Microsoft Corporation

TINYXML 2.5.3

Copyright (C) 2000-2006, Lee Thomason

VISUAL STUDIO CRT SOURCE CODE 8.0

Copyright (C) Microsoft Corporation

WINDOWS TEMPLATE LIBRARY 8.0

Copyright (C) Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

ZLIB 1.0.4, 1.0.8, 1.2.2, 1.2.3

Copyright (C) 1995-2010, Jean-loup Gailly and Mark Adler

DEVELOPMENT TOOLS

Third-party development tools and other resources were used during the application development.

IN THIS SECTION:

MS DDK 4.0, 2000 264

MS WDK 6000, 6001, 6002 264

WINDOWS INSTALLER XML (WIX) TOOLSET 3.0 264

MS DDK 4.0, 2000

Copyright (C) Microsoft Corporation

MS WDK 6000, 6001, 6002

Copyright (C) 2001-2007, Microsoft Corporation

WINDOWS INSTALLER XML (WIX) TOOLSET 3.0

Copyright (C) Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE

EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

DISTRIBUTED PROGRAM CODE

Independent third-party program code is distributed within the application in original or binary format without any changes.

IN THIS SECTION:

GRUB4DOS 0.4.4-2009-10-16 (FILE GRUB.EXE) 269

SYSLINUX 3.86 (FILE SYSLINUX.EXE) 273

GRUB4DOS 0.4.4-2009-10-16 (FILE GRUB.EXE)

Copyright (C) 1999, 2000, 2001, 2002, 2004, 2005 Free Software Foundation, Inc

---

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of

preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

SYSLINUX 3.86 (FILE SYSLINUX.EXE)

Copyright (C) 1994-2010, H. Peter Anvin et al

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of

preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.  This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

OTHER INFORMATION

Additional information about third-party code.

Agava-C program library, developed by OOO "R-Alpha", is used to check digital signature.

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software.

Crypto C program library, developed by OOO "CryptoEx", http://www.cryptoex.ru, is used to check digital signature.

INDEX

A

Anti-Banner
list of blocked banner addresses 152
Anti-Spam
additional filtering features 146
database of phishing web addresses 140
list of blocked phrases 142
list of blocked senders 143
Microsoft Exchange Server messages 148
plug-in for Microsoft Office Outlook 149
plug-in for Microsoft Outlook Express 149
plug-in for The Bat! 150
plug-in for Thunderbird 150
restoring the default settings 150
severity level 137
training 137
Application Control
application run sequence 120
editing an application rule 118
protection scope 121
Application rule
Firewall 126
Application run sequence
Application Control 120
Application Self-Defense 173

B

Browser Configuration 178

C

Computer performance 171
Context menu 43

D

Data clearing
Safe Run 158
Database of phishing web addresses
Anti-Spam 140
IM Anti-Virus 110
Web Anti-Virus 104
Disabling / enabling real-time protection 53

E

Editing an application rule
Application Control 118
Enable
Parental Control 160

F

File Anti-Virus
heuristic analysis 93
pausing 90
protection scope 91
response to a threat 93

scan mode 92
scan of compound files 94
scan optimization 95
scan technology 93
security level 92

Firewall
application rule 126
changing the network status 124
changing the rule priority 126
Firewall rule 124
packet rule 125

Firewall rule
Firewall 124

H

Heuristic analysis
File Anti-Virus 93
Mail Anti-Virus 98
Web Anti-Virus 104

I

IM Anti-Virus
database of phishing web addresses 110
protection scope 109

Infected object 230

Installation folder 30

K

Kaspersky URL advisor
Web Anti-Virus 106

L

License 231
activating the application 55
active 227
End User License Agreement 39
obtaining a key file 231

License renewal 56

M

Mail Anti-Virus
attachment filtering 98
heuristic analysis 98
protection scope 96
response to a threat 98
scan of compound files 99
security level 97

Main application window 44

N

Network
encrypted connections 130
monitored ports 133

Network Attack Blocker
blocking time 130
types of detected network attacks 128
unblocking the computer 130

Network Monitor 132

Notifications 57
delivery of notifications using email 187

disabling 186
disabling sound signal 187
notifications types 187

P

Packet rule
Firewall 125
Parental Control
browsing websites 164
communicating via IM clients 165
downloading files from the Internet 164
enabling and disabling 160
exporting / importing settings 161
limiting the time of computer use 163
limiting the time of Internet use 163
running applications 163
safe search mode 164
searching for key words 167
sending private data 167
Proactive Defense
dangerous activity list 112
dangerous activity monitoring rule 112
group of trusted applications 111
Protection scope
Application Control 121
File Anti-Virus 91
IM Anti-Virus 109
Mail Anti-Virus 96
Web Anti-Virus 108

Q

Quarantine and Backup 174

R

Reports
events search 182
filtering 181
saving to file 183
selecting a component or a task 181
view 70
Rescue Disk 67
Response to a threat
File Anti-Virus 93
Mail Anti-Virus 98
virus scan 81
Web Anti-Virus 103
Restoring the default settings 70
Anti-Spam 150
Restricting access to the application 76

S

Safe Run
data clearing 158
shared folder 157
Scan
account 81
action on a detected object 81
automatic startup of a skipped task 79
scan of compound files 82
scan optimization 83
scan technologies 81
schedule 79

security level 78
starting the task 58
type of objects to scan 82
vulnerability scan 84

Schedule
update 87
virus scan 79

Security level
File Anti-Virus 92
Mail Anti-Virus 97
Web Anti-Virus 103

Shared folder
Safe Run 157

Software requirements 26

T

Taskbar notification area icon 42

Traces
creating a trace file 195
uploading tracing results 195

Training Anti-Spam
using an email client 139
using outgoing messages 138
using reports 140
using the Training Wizard 138

Trusted zone
exclusion rules 169
trusted applications 169

U

Uninstallation
application 37

Update
proxy server 89
regional settings 86
rolling back the last update 88
update source 85

Updating from a local folder 86

V

Virtual Keyboard 62

W

Web Anti-Virus
database of phishing web addresses 104
Geo Filter 107
heuristic analysis 104
Kaspersky URL advisor 106
protection scope 108
response to a threat 103
Safe Surf 106
scan optimization 105
security level 103